Honeywell

MX9 Mobile Computer

with Microsoft® Windows® Embedded CE 6.0

User's Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

© 2009-2014 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

Trademarks

RFTerm is a trademark or registered trademark of EMS Technologies, Inc. in the United States and/or other countries.

Microsoft® Windows®, ActiveSync®, MSN, Outlook®, Windows Mobile®, the Windows logo, and Windows Media are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Marvell® is a registered trademark of Marvell Technology Group Ltd., or its subsidiaries in the United States and other countries.

Summit Data Communications, the Laird Technologies Logo, the Summit logo, and “Connected. No Matter What” are trademarks of Laird Technologies, Inc.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.

microSD and microSDHC are trademarks or registered trademarks of SD-3C, LLC in the United States and/or other countries.

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Hand Held is a trademark of Hand Held Products, Inc., a subsidiary of Honeywell International.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Wavelink®, the Wavelink logo and tagline, Wavelink Studio™, Avalanche Management Console™, Mobile Manager™, Mobile Manager Enterprise™ are trademarks of Wavelink Corporation, Kirkland, WA.

Wi-Fi®, WMM®, Wi-Fi Mutlimedia™, Wi-Fi Protected Access®, WPA™, WPA2™ and the Wi-Fi CERTIFIED™ logo are trademarks or registered trademarks of Wi-Fi Alliance.

Acrobat® Reader © 2014 with express permission from Adobe Systems Incorporated.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, please refer to www.hsmpats.com.

Table of Contents

Chapter 1 - MX9 Agency Compliance

Laser Warnings 1-1
Laser Label Location 1-1
Laser Safety Statement 1-1

Chapter 2 - Getting Started

Overview 2-1
About this Guide 2-1
Out of the Box 2-1
Initial Setup for MX9 2-1
    Hardware Setup 2-1
    Software Setup 2-2
Components 2-3
    Front View 2-3
    62 Key Keypad 2-4
    38 Key Keypad 2-5
    Top 2-5
    Bottom 2-5
    Back - Battery Bay 2-6
    Trigger Handle 2-6
    Hand Strap 2-7
End User License Agreement 2-7
Inserting or Replacing the Battery Pack 2-7
    Insert/Replace Battery 2-7
    Remove Battery 2-8
    Insert Battery in HazLoc MX9 2-8
    Remove Battery from HazLoc MX9 2-8
Charging/Recharging the Main Battery 2-8
LEDs, Backlights and Indicators 2-9
    Status LEDs 2-9
    System Status LED 2-9
    Battery Charging Status LED 2-9
    Alpha mode Status LED 2-9
    Bluetooth Status LED 2-9
    Keypad Backlight Setting 2-9
    Toggle Vibrate Indicator 2-9
Tapping the Touch Screen with a Stylus 2-9
Calibrating the Touch Screen 2-10
Adjusting the Display Backlight Brightness 2-10
Adjusting the Display Backlight Timer 2-10
Applying the Touch Screen Protective Film 2-10
Adjusting the Keypad Backlight 2-11
Setting Date and Time Zone 2-11
    Grab Time Utility 2-11
    Autolaunch Time-Sync 2-11
    Synchronize with a Local Time Server 2-11
Setting Power Scheme Timers 2-12
    Battery Power Scheme 2-12

AC Power Scheme....2-12
Setting Speaker Volume....2-13
Using the Keypad....2-13
Using a Control Panel....2-13
Body Worn Accessories....2-14
Holster without Handle....2-14
Holster with Handle....2-14
Carrycase....2-14
Using the Input Panel / Virtual Keyboard....2-15
Connecting Bluetooth Devices....2-15
Bluetooth On-Screen Indicator....2-16
Bluetooth LED Functions....2-16
Setting Terminal Emulation Parameters....2-16
Using the AppLock Switchpad....2-17
Using the Keypad....2-17
Using the Touch Screen....2-17
Rebooting the MX9....2-17
Warmboot....2-17
Restart (or Cold Boot)....2-17
Installing the SIM Card....2-18
Attaching the Hand Strap....2-19
Attaching the Trigger Handle....2-20
Adjusting the Headset / Microphone and Securing the Cable....2-21
Connecting Cables to the MX9....2-22
Connecting the USB Host and Power Cable....2-22
Connecting the USB Client and Power Cable....2-22
Connecting the Serial and Power Cable....2-23
Connecting an External Power Supply....2-23
Replacing the CLA Fuse....2-24
Cleaning the Touch Screen and Scanner Aperture....2-24
Startup Help....2-25

Chapter 3 - Hardware Configuration

802.11 b/g and a/b/g Wireless Client....3-1
Central Processing Unit....3-1
System Memory....3-1
Internal SD Memory Card....3-1
Video Subsystem....3-1
Power Supply....3-1
Input/Output Connector....3-2
Audio Support....3-2
Bluetooth....3-2
Keypads....3-3
Modifier Keys....3-3
Expansion Slots....3-3
Power Key Functions....3-4
Status LEDs....3-4
System Status LED....3-4
Battery Charging Status LED....3-4
Alpha mode Status LED....3-4

Bluetooth Status LED 3-4
Scanner Status LED....3-5
Cold Storage....3-5
Vibrate Indicator 3-5
Scanners and Imagers 3-6
Integrated Bar Code Decoders 3-6
Tethered Bar Code Decoders 3-6
Bluetooth Client Bar Code Decoders 3-6
GPS Module 3-6

Chapter 4 - Power Modes and Batteries

Power Modes....4-1
On 4-1
User Idle....4-1
System Idle 4-1
Wake Up Event Default Settings 4-2
Critical Suspend....4-2
Off 4-2
Batteries 4-3
Checking Battery Status....4-3
Main Battery Pack....4-3
Battery Hotswapping....4-3
Low Battery Warning....4-3
Super-cap Internal Battery 4-3
Handling Batteries Safely....4-4
External Power Supplies 4-4
AC/DC 15V Power Supply 4-4
Car Power Adapter....4-4

Chapter 5 - Software Configuration

Introduction....5-1
Operating System....5-1
Windows CE Operating System 5-1
General Windows CE Keyboard Shortcuts 5-1
Warmboot....5-2
Clearing Persistent Storage / Reset to Default Settings 5-2
Folders Copied at Startup 5-2
Saving Changes to the Registry....5-2
Software Load 5-3
Software Applications....5-3
Bluetooth (Optional) 5-3
RFTerm (Optional) 5-3
Avalanche 5-3
Software Development....5-3
Accessing Files on the SD/CF Card....5-3
Utilities....5-4
LAUNCH.EXE....5-4
LAUNCH.EXE and Persistent Storage 5-4
REGEDIT.EXE 5-5

REGLOAD.EXE 5-5
REGDUMP.EXE 5-5
WARMBOOT.EXE 5-5
WAVPLAY.EXE 5-5
MX9 Command-line Utilities 5-5
PrtScrn.EXE 5-5
Desktop 5-6
Desktop Icons 5-6
Taskbar 5-6
My Device Folders 5-7
Wavelink Avalanche Enabler (Optional) 5-7
Internet Explorer 5-7
Start Menu Program Options 5-8
Communication 5-8
ActiveSync 5-8
Connect and HSM Connect (or LXEConnect) 5-8
Start FTP Server / Stop FTP Server 5-8
Summit 5-9
Certs 5-9
Command Prompt 5-9
eXpress Scan 5-9
Internet Explorer 5-9
Microsoft WordPad 5-9
Remote Desktop Connection 5-9
Settings 5-10
Transcriber 5-10
Windows Explorer 5-10
Taskbar 5-11
General Tab 5-11
Advanced Tab 5-11
Taskbar Icons 5-12
Upgrading the Operating System 5-13
Introduction 5-13
Updates and Language Options 5-13
Preparation 5-13
Accessing the SD Card Slot 5-13
Procedure 5-13
Upgrade Help 5-14
Battery State and OS Upgrade 5-14
Control Panel 5-15
About 5-17
Version Tab and the Registry 5-17
Languages 5-17
Identifying Software Versions 5-17
MAC Address 5-17
Accessibility 5-18
Battery 5-19
Certificates 5-20
Date / Time 5-21
Device Management 5-22
Dialing 5-22
Display 5-23

Background 5-23
Appearance 5-24
Backlight 5-25
Input Panel 5-26
Internet Options 5-27
Keyboard 5-30
KeyMap 5-31
KeyMap Tab 5-32
Remap a Single Key 5-32
Remap a Key to a Unicode Value 5-32
Remap a Key Sequence 5-32
Remap a Key to a Sequence of Unicode Values 5-33
Remap an Application 5-33
Remap a Command 5-33
LaunchApp Tab 5-34
RunCmd Tab 5-35
License Viewer 5-36
Mixer 5-37
Output Panel 5-37
Input Panel 5-38
Mouse 5-38
MX9 Options 5-39
Communication Tab 5-39
Misc Tab 5-40
Status Popup Tab 5-41
Network and Dialup Options 5-42
Creating a New Connection 5-42
Network Capture 5-43
Netlog Tab 5-43
NDISlog Tab 5-45
Owner 5-46
Password 5-48
PC Connection 5-49
Peripherals 5-50
Heaters Tab 5-50
Flashlight Tab 5-51
GPS Tab 5-51
Power 5-52
Regional and Language Settings 5-54
Registry 5-56
Remove Programs 5-57
Stylus 5-58
System 5-59
General Tab 5-59
Memory Tab 5-60
Device Name Tab 5-60
Copyrights Tab 5-61
Terminal Server Client Licenses 5-62
Volume and Sounds 5-63
Good Scan and Bad Scan Sounds 5-63
Wi-Fi 5-64
WWAN 5-64
Initial Setup 5-65

Connection Tab 5-65
Network Tab 5-66
TCP/IP Tab 5-67
Security Tab 5-68
Autoconnect Tab 5-69
Admin Tab 5-70
About Tab 5-71
Using ActiveSync 5-72
MX9 without Touch Screen 5-72
Initial Setup 5-72
Connect via USB 5-72
Cable for USB ActiveSync Connection 5-73
Serial Connection 5-73
Cable for Serial ActiveSync Connection 5-73
Wireless Connection 5-73
Synchronizing from the Mobile Device 5-74
Explore 5-74
Backup Data Files using ActiveSync 5-74
Serial Port Transfer 5-74
USB Transfer 5-74
Connect 5-74
Disconnect 5-74
USB Connection 5-74
Serial Connection 5-75
Network Connection 5-75
ActiveSync Help 5-75
Cold Boot and Loss of Host Re-connection 5-76
Configuring the MX9 with HSM Connect (or LXEConnect) 5-77
Installing HSM Connect (or LXEConnect) 5-77
Using HSM Connect (or LXEConnect) 5-77

Chapter 6 - AppLock

Introduction 6-1
Setup a New Device 6-1
Administration Mode 6-2
End User Mode 6-2
Passwords 6-3
AppLock Password Help 6-3
End-User Switching Technique 6-3
Using a Stylus Tap 6-3
Using the Switch Key Sequence 6-3
Hotkey (Activation hotkey) 6-4
End User Internet Explorer (EUIE) 6-4
Application Configuration 6-5
Application Panel 6-5
Launch Button 6-7
Auto At Boot 6-7
Auto Re-Launch 6-8
Manual (Launch) 6-8
Match 6-8

Allow Close 6-9
Security Panel 6-9
Setting an Activation Hotkey 6-9
Setting a Password in the Security Panel 6-10
Options Panel 6-10
Status Panel 6-11
View 6-11
Log 6-12
Save As 6-12
AppLock Help 6-12
AppLock Error Messages 6-13

Chapter 7 - Bluetooth Configuration

Introduction 7-1
Initial Configuration 7-3
Subsequent Use 7-3
Bluetooth Devices 7-4
Clear Button 7-4
Discover Button 7-4
Discovering 7-5
Stop Button 7-5
Bluetooth Device List 7-6
Bluetooth Device Menu 7-7
Bluetooth Properties 7-8
Settings 7-8
Turn On Bluetooth (Button) 7-8
Options 7-8
Reconnect 7-10
Options 7-10
About 7-11
Easy Pairing and Auto-Reconnect 7-12
Bluetooth Indicators 7-12
Bluetooth Bar Code Reader Setup 7-12
Introduction 7-12
MX9 with Label 7-13
MX9 without Label 7-13
Bluetooth Reader Beep and LED Indications 7-14
Bluetooth Printer Setup 7-14
Using OPP 7-15
Pairing with an OPP Device 7-15
Remote Device Pushes File to MX9 7-15
MX9 Pushes File to Remote Device 7-16
EZPair (or LXEZ Pairing) and External Applications 7-16
OPP Setup Tab 7-16
OPP Send Tab 7-18
Buttons 7-18

Chapter 8 - Data Collection Wedge

Introduction 8-1

Return to Factory Default Settings 8-1
Data Processing Overview 8-2
Main Tab....8-3
Continuous Scan Mode....8-4
COM1 Tab 8-5
Notification Tab....8-6
Data Options Tab 8-7
Enable Code ID....8-8
Symbology Settings 8-9
Processing Order 8-10
Strip Leading/Trailing Control....8-11
Barcode Data Match List....8-12
Add Prefix/Suffix Control 8-13
Symbologies....8-14
AIM Symbologies....8-14
HHP Symbologies 8-15
Advanced Button (Hand Held Products Imager Only) 8-15
Codabar - Advanced Properties 8-16
Code 11 - Advanced Properties 8-16
Code 39- Advanced Properties 8-17
EAN 8 - Advanced Properties 8-18
EAN 13 - Advanced Properties 8-19
Interleaved 2 of 5 - Advanced Properties 8-19
Mesa - Advanced Properties 8-20
MSI Plessy - Advanced Properties 8-21
OCR Properties - Advanced Properties 8-22
Planet - Advanced Properties 8-23
Posicode - Advanced Properties 8-24
Telepen - Advanced Properties 8-24
UPCA - Advanced Properties 8-25
UPCE0 - Advanced Properties 8-26
UPCE1 - Advanced Properties 8-27
HHP Properties 8-28
Ctrl Char Mapping 8-30
Translate All 8-30
Custom Identifiers....8-31
Control Code Replacement Examples....8-32
Bar Code Processing Examples....8-33
Length Based Bar Code Stripping....8-34
Processing Tab....8-36
About Tab 8-37
Hat Encoding 8-38

Chapter 9 - Enabler Installation and Configuration

Introduction....9-1
Installation 9-1
Installing the Enabler 9-1
Enabler Uninstall Process 9-2
Stop the Enabler Service....9-2
Update Monitoring Overview 9-2

Mobile Device Wireless and Network Settings 9-2
Preparing a Device for Remote Management 9-3
User Interface 9-4
Enabler Configuration 9-4
File Menu Options 9-5
Avalanche Update using File > Settings 9-6
Menu Options 9-6
Connection 9-7
Execution 9-8
Server Contact 9-8
Data 9-9
Preferences 9-11
Taskbar 9-12
Scan Config 9-13
Display 9-14
Shortcuts 9-15
SaaS 9-16
Adapters 9-17
Status 9-19
Exit 9-20
Using Remote Management 9-21
Using eXpress Scan 9-21
Creating Bar Codes 9-21
Scanning Bar Codes 9-21
Process Complete 9-22

Chapter 10 - Wireless Network Configuration

Introduction 10-1
Important Notes 10-1
Summit Client Utility 10-1
Help 10-1
Summit Tray Icon 10-2
Wireless Zero Config Utility and the Summit Radio 10-3
Using the Wireless Zero Config Utility 10-3
Switching Control to SCU 10-3
Main Tab 10-3
Auto Profile 10-4
Admin Login 10-4
Profile Tab 10-6
Buttons 10-6
Profile Parameters 10-8
Status Tab 10-10
Diags Tab 10-11
Global Tab 10-12
Custom Parameter Option 10-13
Global Parameters 10-13
Sign-On vs. Stored Credentials 10-17
Using Stored Credentials 10-17
Using a Sign On Screen 10-17
Windows Certificate Store vs. Certs Path 10-19
User Certificates 10-19

Root CA Certificates....10-19
Using the Certs Path....10-19
Using the Windows Certificate Store....10-19
Configuring Profiles....10-21
No Security....10-21
WEP....10-22
LEAP....10-23
PEAP/MSCHAP....10-24
PEAP/GTC....10-26
WPA/LEAP....10-28
EAP-FAST....10-29
EAP-TLS....10-31
WPA PSK....10-33
Certificates....10-34
Generating a Root CA Certificate....10-34
Installing a Root CA Certificate....10-37
Generating a User Certificate....10-38
Installing a User Certificate....10-44
Verify Installation....10-47

Chapter 11 - KeyMaps

Introduction....11-1
62-Key Keypad KeyMap....11-1
62-Key 5250 Keypad Overlay KeyMap....11-6
38-key Keypad KeyMap....11-11

Chapter 12 - Battery Charger

Unpacking your Battery Charger....12-1
Introduction....12-1
Cautions and Warnings....12-2
Battery Charger....12-2
Lithium-Ion Battery Pack....12-2
Front View....12-3
Installation....12-3
Assemble the Power Supply....12-3
Setup....12-4
Mounting....12-4
Charging Batteries....12-4
Inserting a Battery into the Charging Pocket....12-5
Removing the Battery from the Charging Pocket....12-5
Interpreting the Charging Pocket LEDs....12-5
Battery Charger Help....12-6
Charger Cleaning, Storage and Service....12-7
Cleaning....12-7
Storage....12-7
Service....12-7
Battery Cleaning, Storage and Service....12-7
Cleaning....12-7

Storage....12-7
Service....12-8

Chapter 13 - Cradles

Unpacking your Cradles....13-1
Overview....13-1
Preparing the Cradle for Use....13-1
Tethered Scanners and the MX9 Cradles....13-2
Cradle Cleaning, Storage and Service....13-2
Battery Cleaning, Storage and Service....13-3
Using a Desktop Cradle....13-3
Introduction....13-3
Quick Start - Desktop Cradle....13-3
Battery Charging in a Desktop Cradle....13-3
Front View....13-4
Back View....13-4
Side View....13-4
Top View....13-5
Desktop Mounting Footprint....13-5
Assemble/Attach the AC Power Adapter....13-6
Connecting Input/Output and Power Cables to the Desktop Cradle....13-6
Desktop Cradle Connector Identifiers....13-7
Connecting a Headset Audio Cable....13-7
Connecting the Power Cable....13-7
Connecting a Serial Cable....13-7
Connecting an Ethernet RJ-45 Cable....13-7
Connecting a USB Host and USB Client Cable....13-7
Cradle LEDs....13-7
Docked LED....13-7
Spare Battery LED....13-8
MX9 System Status LED Status when Docked....13-8
Docking and Undocking the MX9....13-8
Dock the MX9....13-8
Undock the MX9....13-8
Inserting / Removing a Spare Battery from the Desktop Cradle....13-8
Inserting a Spare Battery....13-9
Removing a Spare Battery....13-9
Desktop Cradle Help....13-9
Using a Powered Vehicle Cradle....13-11
Introduction....13-11
Quick Start - Vehicle Cradle....13-11
Components....13-12
Front View....13-12
Back View....13-12
RAM Bracket Mounting....13-13
RAM Bracket Mounting Points....13-13
Vehicle Cradle RAM Ball Assembly....13-14
RAM Circular Base Footprint....13-14
DC/DC Power Supply Installation, Screws on Side of Lid....13-15
Connecting Electrical Cables to Power Sources....13-15
Specifications for Electrical Supply....13-15

Wiring Schematic....13-16
Connecting to Vehicle Power....13-16
DC/DC Power Supply Installation, Screws on Top of Lid....13-18
Connecting Electrical Cables to Power Sources....13-18
Specifications for Electrical Supply....13-18
Wiring Schematic....13-19
Connecting Vehicle Electrical Supply....13-19
Vehicle 12V Bare Wire Adapter....13-21
Vehicle Cable Connection (Fuse Not Shown)....13-21
Connecting the Power Cable to the Vehicle....13-21
Connecting Vehicle 12 VDC Supply....13-22
Connecting Power Supply to Vehicle Cradle....13-22
Attaching a Serial or I/O Connector....13-22
Serial Interface....13-22
I/O Port....13-23
Vehicle Cradle Strain Relief Cable Clamp....13-23
Vehicle Cradle LED....13-24
Docking the MX9 in a Vehicle Mounted Cradle....13-24
Removing the MX9 from the Mounted Vehicle Cradle....13-25
Powered Vehicle Cradle Help....13-25

Chapter 14 - Technical Specifications

MX9 Specifications....14-1
MX9 Dimensions and Weight.....14-1
MX9 Environmental Specifications....14-2
Main Battery Technical Specifications....14-2
Wireless Radio....14-2
Bluetooth System Compatibility....14-3
WWAN Radio....14-3
AC/DC Wall Adapter (for MX9, Desktop Cradle, Battery Charger)....14-3
GPS Receiver Technical Specifications....14-3
Desktop and Vehicle Cradle Pinout - RS232 Connector....14-4
Desktop Cradle Technical Specifications....14-5
Battery Charger Technical Specifications....14-5
Electrical....14-5
Temperature....14-5
Dimensions....14-6

Chapter 15 - Customer Support

Technical Assistance....15-1
Product Service and Repair....15-1
Limited Warranty....15-1

1

MX9 Agency Compliance

MX9 mobile computers meet or exceed the requirements of all applicable standards organizations for safe operation. However, as with any electrical equipment, the best way to ensure safe operation is to operate them according to the agency guidelines that follow. Read these guidelines carefully before using your MX9.

This documentation is relevant for the following models: MX9, MX9CS, MX9HL.

Caution:



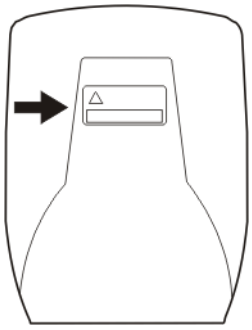
RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. The battery should be disposed of by a qualified recycler or hazardous materials handler. Do not incinerate the battery or dispose of the battery with general waste materials.

Laser Warnings

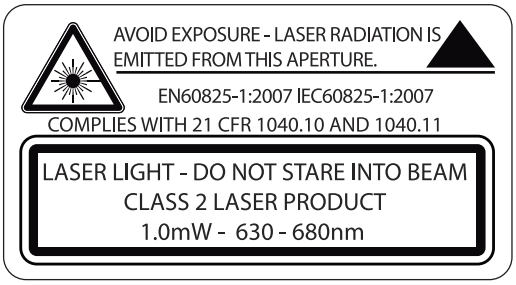
- Do not look into the laser's lens.
- Do not stare directly into the laser beam.
- Do not remove the laser caution labels from the MX9.
- Do not connect the laser bar code aperture to any other device. The laser bar code aperture is certified for use with the MX9 only.

Caution: 	Laser radiation when open. Read the caution labels. Use of controls, adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Laser Label Location



f the following label is attached to your MX9, it indicates the MX9 contains an engine with a laser aimer:


AVOID EXPOSURE - LASER RADIATION IS EMITTED FROM THIS APERTURE.
EN60825-1:2007 IEC60825-1:2007
COMPLIES WITH 21 CFR 1040.10 AND 1040.11
LASER LIGHT - DO NOT STARE INTO BEAM
CLASS 2 LASER PRODUCT
1.0mW - 630 - 680nm

Laser Safety Statement

This device has been tested in accordance with and complies with IEC60825-1 ed2 (2007). Complies with 21 CFR 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

LASER LIGHT, DO NOT STARE INTO BEAM, CLASS 2 LASER PRODUCT, 1.0 mW MAX OUTPUT: 630-680nM.

Model Number, Serial Number and IMEI Labels

The model (item) number, serial number, and international mobile equipment identity (IMEI) number for the terminal are located on labels affixed to the back of the terminal.

FCC Part 15 Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet helpful: “Something About Interference.” This is available at FCC local regional offices. Honeywell is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Honeywell. The correction is the responsibility of the user.

Caution: Any changes or modifications made to this equipment not expressly approved by Honeywell may void the FCC authorization to operate this equipment.

FCC 5GHz Statement

LAN devices are restricted to indoor use only in the band 5150-5250 MHz. For the band 5600-5650 MHz, no operation is permitted.

When using IEEE 802.11a wireless LAN, this product is restricted to indoor use, due to its operation in the 5.15- to 5.25-GHz Frequency range. The FCC requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High-power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65- to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

Canadian Compliance

This ISM device complies with Canadian RSS-210.

Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

CE Mark

The CE marking indicates compliance with the following directives:

- 1995/5/EC R&TTE
- 2011/65/EU RoHS (Recast)

In addition, complies to 2006/95/EC Low Voltage Directive, when shipped with recommended power supply. European contact::

CE

Hand Held Products Europe BV
Nijverheidsweg 9-13
5627 BT Eindhoven
The Netherlands

Honeywell shall not be liable for use of our product with equipment (i.e., power supplies, personal computers, etc.) that is not CE marked and does not comply with the Low Voltage Directive.

RF Notices

This device can contain transmitter Module(s) FCC ID: DDZLXE4830P, KDZBT001, E09HHSR3. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment under 47 CFR 2.1093 paragraph (d)(2).

FCC / EU RF Exposure Guidelines

Safety Information

The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices.

Reducing RF Exposure - Use Properly

It is advisable to use the device only in the normal operating position.

Handheld Devices

This device was tested for typical body-worn operation. Use only Honeywell tested and approved accessories to ensure FCC Compliance. The use of third-party accessories may not comply with FCC RF exposure compliance requirements, and should be avoided. To comply with FCC RF exposure requirements, this device must be operated in the hand with a minimum separation distance of 2.5 cm (0.9842 inch) or more from a person's body or with the following body-worn accessories as shown in the applicable section of the manual, see Body Worn Accessories (page 2-14).

- MX9420HOLSTER

- MX9423HOLSTER

- MX9410CASE. Shoulder strap is not approved with use with WWAN configurations.

Bluetooth

Bluetooth® Class II

Honeywell Scanning & Mobility Product Environmental Information

Refer to www.honeywellaidc.com/environmental for the RoHS / REACH / WEEE information.

Dealer License - Republic of Singapore

Complies with
IDA Standards
DA103458

Vehicle Power Supply Connection Safety Statement

Vehicle Power Supply Connection: If the supply connection is made directly to the battery, a 10A slow-blow fuse should be installed in the positive lead within 5 inches (12.7 cm) of the battery positive (+) terminal.

Brazil Restrictions

Bluetooth and GSM technology are not available in Brazil.

In Brazil the MX9 is not available with the MX9 AC/DC power adapter and MX9 Desktop cradle.

2 Getting Started

Overview

The MX9 is a ruggedized handheld computer targeted for indoor and outdoor use. It is powered by a lightweight main battery that can be removed and replaced without the need for special tools.

MX9 wireless connectivity is secured by user-configured encryption and authentication protocols. The MX9 has an integrated keyboard, outdoor readable touch display, a tethered stylus, Microsoft® Windows® operating system, and many wireless connection options.

The keypad is available in a 62-key or 38-key configuration. The 62-key keypad is also available in an IBM 5250 configuration. Bar code reader options are: an imager or laser scanner integrated in the MX9, or a handheld scanner tethered to the port at the base of the MX9, Bluetooth mobile bar code imagers and scanners, or the Bluetooth Ring Scanner module.

Wireless network connection is accomplished using a Summit WLAN 802.11 radio, WWAN, and Bluetooth. Desk and vehicle cradles, a trigger handle or hand strap, holsters with shoulder straps or belts, clear covers for cases and holsters, Bluetooth scanners and printer, standard and low temperature batteries, and battery chargers are among the many accessories available for the MX9.

About this Guide

This MX9 User's Guide provides instruction for the system administrator to follow when configuring a MX9 with a Microsoft Windows CE 5 operating system. Also included are setup and use instructions for the MX9 Battery Charger, Desktop Cradle, and Powered Vehicle Mounted Cradle.

Out of the Box

After you open the shipping carton verify it contains the following items:

- MX9 Hand Held Computer
- Rechargeable battery
- Hand Strap (attached to the MX9)
- Quick Start Guide

If you ordered accessories for the MX9, verify they are also included with the order. Keep the original packaging material in the event the MX9 should need to be returned for service. For details, see Product Service and Repair (page 15-1).

Initial Setup for MX9

Following are steps you might take when setting up a new MX9. Follow the links for further instruction for each step. Contact Technical Assistance (page 15-1) if you need additional help.

Note: Installing or removing accessories should be performed on a clean, well-lit surface. When necessary, protect the work surface, the MX9, and components from electrostatic discharge.

While the MX9 is in a hazardous location DO NOT:

- Connect an external power source to the MX9.
- Connect a USB device or audio jack to the MX9.
- Connect the Car Power Adapter to the I/O connector at the base of the MX9.
- Remove or install a battery pack in the MX9.

Hardware Setup

1. Connect accessories e.g., hand strap (if necessary), trigger handle, etc.
2. Provide a power source:
   - Insert a fully charged main battery.
   - Connect a power cable (USB/Power or Serial/Power).
   - Place the MX9 in a powered desktop or vehicle mounted cradle.
3. Press the Power key.

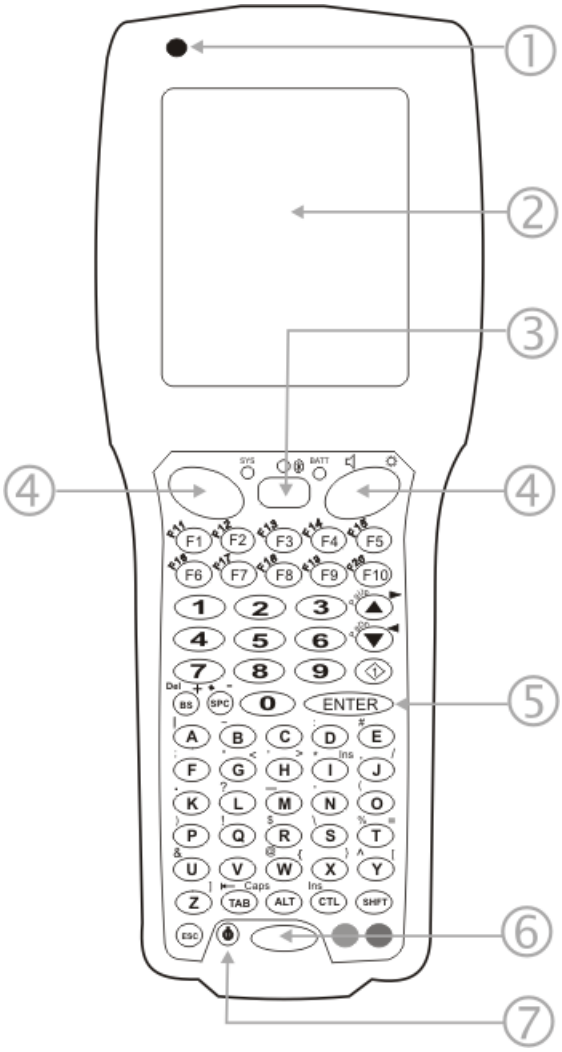
Software Setup

Hardware setup should be completed before starting software setup.

1. Calibrate touch display.
2. Set Date and Time Zone.
3. Set Power Timers.
4. Set Speaker Volume.
5. Pair Bluetooth devices.
6. Set Wireless client parameters.
7. Set terminal emulation parameters.
8. Set AppLock parameters.
9. Set DCWedge parameters.

Components

Front View

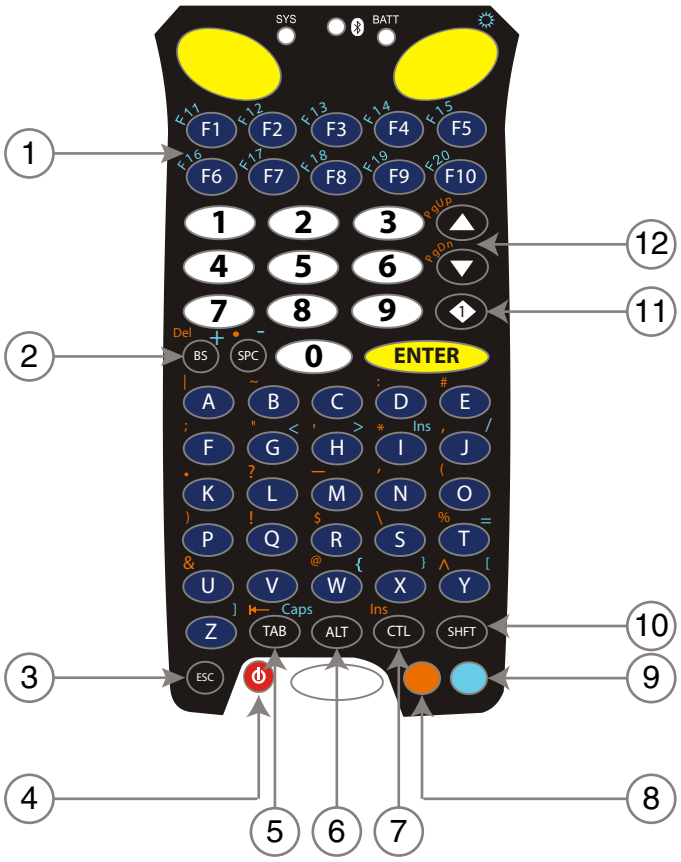


1. Microphone
2. Touch screen
3. Speaker
4. Scan buttons
5. Enter key
6. Scanner status LED
7. Power key

The above list is the same on the 38 key MX9.

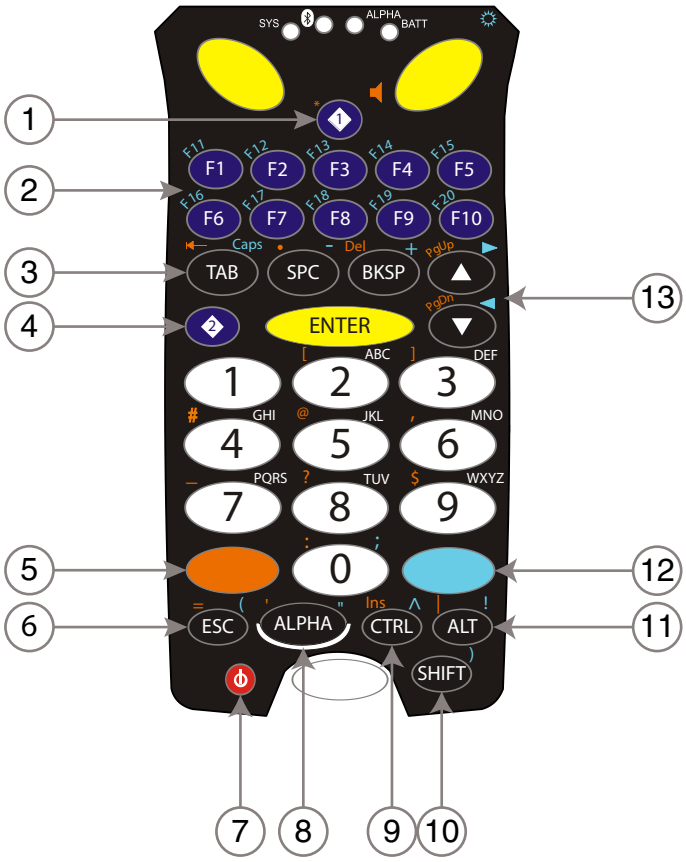
Special keys are listed on the following pages.

62 Key Keypad



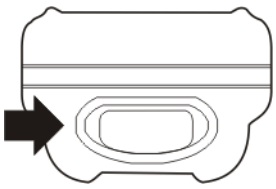
1. Function Keys
2. Backspace [BS] key and Space [SPC] key
3. Escape [ESC] key
4. Power key
5. Tab key
6. Alt key
7. Control [CTL] key
8. Orange key
9. Blue key
10. Shift [SHFT] key
11. Diamond 1 key
12. Cursor up and down Keys

38 Key Keypad



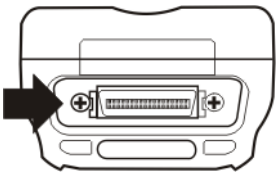
1. Diamond 1 key
2. Function keys
3. Tab | Space | Backspace keys
4. Diamond 2 key
5. Orange key
6. Escape [ESC] key
7. Power key
8. Alpha key
9. Control [CTRL] key
10. Shift [SHIFT] key
11. Alt key
12. Blue key
13. Cursor up and down keys

Top



Bar code reader aperture

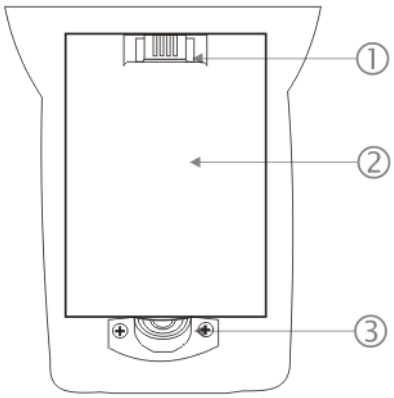
Bottom



Input / Output Connector

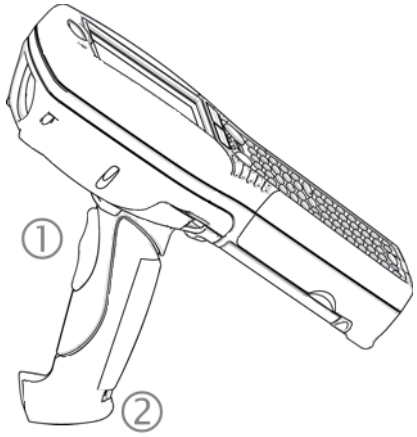
Tethered boot cover (covers I/O connector) not shown

Back - Battery Bay

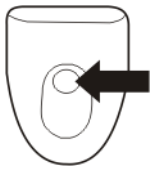


1. Battery Charging Terminals
2. Battery Bay
3. Battery Bay Access Tab

Trigger Handle

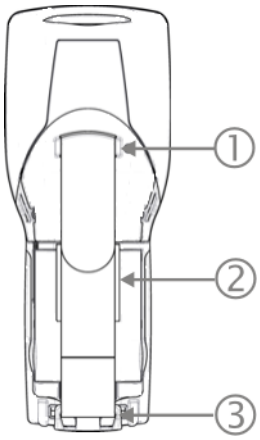


1. Trigger
2. Tether attach point



Stylus storage bay in trigger handle base

Hand Strap



1. Hand strap connector, upper
2. Stylus holder on Hand strap
3. Hand strap connector, lower

End User License Agreement

When a new MX9 starts up a EULA is displayed on the touch screen. It remains on the screen until the Accept or Decline button is tapped with a stylus.

- Tap the Accept button to accept the EULA terms and the MX9 continues the startup process. The EULA is not presented to the user again.
- Tap the Decline button to decline the EULA and the MX9 will reboot. It will continue to reboot until the Accept button is tapped with the stylus.

Note: The EULA will be presented after any operating system upgrade or re-installation, including language-specific operating systems.

Inserting or Replacing the Battery Pack

Warning: Never remove or replace any battery in a hazardous location.

The MX9 will not function unless the battery pack is in place and securely latched.

Be sure to place the unit in Suspend Mode before removing the battery. Failing to properly place the device in Suspend mode will result in a loss of all unsaved data.

The main battery is located in a compartment on the back of the unit. The battery case serves as the back cover for the battery well of the MX9.

An MX9 will retain data, while the main battery is removed and replaced with a fully charged main battery, for 5 minutes.
Important: When the internal battery power is Low or Very Low connect the AC adapter to the MX9 before replacing the main battery.

Note: The battery should not be replaced in a dirty, harsh or hazardous environment. When the battery is not connected to the MX9, any dust or moisture that enters the battery well or connector may transfer to the battery/well terminals, potentially causing damage.

Warning. Only use Honeywell batteries as replacements: MX9380BATTERY 161888-0001 or 161915-0001 (Low Temperature)

Insert/Replace Battery

To insert the main battery, complete the following steps:

1. Detach the bottom hook of the hand strap (if installed).
2. Tilt the end (with the terminals) of the fully charged battery pack into the upper end of the battery compartment, and firmly press the other end until it is fully inserted into the battery compartment.
3. Push down on the battery until the retaining clip clicks into place.
4. Replace the hand strap clip in its holder (if installed).

The MX9 draws power from the battery immediately upon successful connection.

Check battery status in the Battery control panel.

Remove Battery

To remove the battery, complete the following steps:

1. Place the MX9 in Suspend mode.
2. Detach the bottom hook of the hand strap (if installed).
3. Slide the battery retaining clip down to release the main battery.
4. Pull the battery up and out of the battery well with a hinge motion.
5. Place the discharged battery pack in a powered MX9 battery charger.

Insert Battery in HazLoc MX9

1. Detach the bottom hook of the hand strap (if installed).
2. Tilt the end (with the terminals) of the fully charged battery pack into the upper end of the battery compartment, and firmly press the other end until it is seated into the battery compartment.
3. Push down on the battery pack until it clicks into place.
4. Place the **tethered plastic locking tab** over the battery latch, matching up the screw holes in the MX9 body and the screw holes in the tethered plastic locking tab.
5. Using a flat head screwdriver, secure the battery in the battery well by securing the locking screws to the MX9 body.
6. Replace the hand strap clip in its holder.

Remove Battery from HazLoc MX9

1. Place the MX9 in Suspend mode.
2. Detach the bottom hook of the hand strap (if installed).
3. Using a flat head screwdriver, unfasten the **tethered plastic lock**'s captive locking screws.
4. Place the tethered plastic locking tab to one side. Do not remove or unfasten the tether.
5. Slide the battery locking tab down to release the battery pack.
6. Pull the battery up and out of the battery well with a hinge motion.
7. Place the discharged battery pack in a powered MX9 battery charger.

Charging/Recharging the Main Battery

Warning. Only use Honeywell batteries as replacements: MX9380BATTERY 161888-0001 or 161915-0001 (Low Temperature)

Note: The MX9 Battery Charger is designed for an indoor, protected environment. It is not authorized for use in areas designated as Hazardous Locations.

New batteries must be fully charged prior to use.

The main battery can be recharged in an AC powered Battery Charger after the battery has been removed from the MX9 or its packing material when new.

The main battery while in the MX9 can be recharged using several different methods.

Note: An external power source is required before the main battery in the MX9 will recharge.

The main battery can be recharged while it is in the MX9:

- by connecting the MX9 AC power adapter to the I/O connector at the base of the MX9.
- by docking the MX9 in a powered desk cradle
- by docking the MX9 in a powered vehicle cradle

- or by connecting the car power adapter (CLA) to the I/O connector at the base of the MX9.

Note: An uninterrupted external power source (wall AC adapters) transfers power to the computer's internal charging circuitry which, in turn, recharges the main battery and internal battery. Frequent connection to an external power source, if feasible, is recommended to maintain internal battery charge status as the internal battery cannot be recharged by a dead or missing main battery.

LEDs, Backlights and Indicators

Status LEDs

Several LEDs are located on the front of the MX9 above the speaker. They are:

- System Status (SYS) LED indicates power management status (far left LED).
- Battery Charging Status (BATT) LED indicates main battery charging status (far right LED).
- Alpha Mode Status LED applies to the 38-key keypad only (LED is next to SYS LED).
- Bluetooth Status LED applies to Bluetooth client functions (LED is next to BATT LED).

System Status LED

Blinking Red	Battery power fail; critical suspend
Solid Red	Main battery low
Yellow / Amber	Initial few seconds when Power key is pressed

Battery Charging Status LED

Off	No battery, no AC power, battery pack not plugged in or no AC power applied
Flashing Red	Fault, battery pack fault or failure
Yellow / Amber	Standby, battery pack temperature out of range
Red	Charging, battery pack charging (icon on touch screen)
Green	Charged, battery pack fully charged. Connected to external power.

Alpha mode Status LED

- Green when in alpha mode, 38-key keypad only.

Bluetooth Status LED

- Blue when Bluetooth activated
- Off when Bluetooth not activated.

Keypad Backlight Setting

The keypad backlight is white and can be set to be on or off. The default value is on.

When set to off, the keypad backlight does not turn on during Suspend/Restart or reboots.

When set to on, the keypad backlight follows the display backlight settings. The keypad backlight turns off when the display backlight dims.

Toggle Vibrate Indicator

The MX9 vibration motor is activated when a scan is completed successfully (good scan vibration) or with a failure (scan key released before good scan, timeout, or rejected because of Data Options configuration).

The vibrations can be detected under the hand strap or through the trigger handle.

Toggle the vibrate indicator on or off by tapping the desired radio button for Good Scan Vibration and Bad Scan Vibration.

Options are: Off, Short, Medium or Long.

Tapping the Touch Screen with a Stylus

Note: Always use the point of the stylus for tapping or making strokes on the touch screen.

Never use an actual pen, pencil, or sharp/abrasive object to write on the touch screen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. Firmly press the stylus into the stylus holder when the stylus is not in use.

Using a stylus is similar to moving the mouse pointer then left-clicking icons on a desktop computer screen. Using the stylus to tap icons on the touch screen is the basic action that can:

- Open applications
- Choose menu commands
- Select options in dialog boxes or drop-down boxes
- Drag the slider in a scroll bar
- Select text by dragging the stylus across the text
- Place the cursor in a text box prior to typing in data
- Place the cursor in a text box prior to retrieving data using a scanner/imager or an input/output device connected to a serial port.

A right-click can be simulated by touching the touch screen with the stylus and holding it for a short time. A stylus replacement kit is available.

Calibrating the Touch Screen

If the touch screen is not responding properly to stylus taps, you may need to recalibrate the touch screen.

Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To recalibrate the screen, select **Start > Settings > Control Panel > Stylus > Calibration** tab. To begin, tap the Recalibrate button on the screen with the stylus.

Follow the instructions on the screen.

Adjusting the Display Backlight Brightness

When the display backlight is on, press the Blue key and then press either Scan key.

- Use the Up Arrow and Down Arrow keys to adjust backlight brightness until the display lightens or darkens to your satisfaction.
- Press any key, except the up arrow or down arrow keys, to exit this mode.

At the minimum dimness level, the display is still viewable. The brightness setting is recalled upon a return from Suspend and also upon a warm reset/boot.

Note: The brightness of the keypad backlight is not affected by display brightness adjustments or the display brightness default setting.

Adjusting the Display Backlight Timer

The backlight settings use the Honeywell set of default timeouts and are synchronized to the User Idle setting in the Schemes tab in the Power control panel. When the backlight timer expires, the display backlight is dimmed, not turned off. When both check boxes are unchecked, the backlight never turns off (or dims). Default values are 3 seconds for Battery, 2 minutes for External and both the check boxes are enabled. When the keypad backlight is set to *Follow the touch screen backlight*, the keypad backlight turns off when the touch screen backlight dims.

Applying the Touch Screen Protective Film

First, clean the touch screen of fingerprints, lint particles, dust and smudges.

Remove the protective film from its container. Remove any protective backing from the film sheet by lifting the backing from a corner of the film. Discard the backing.

Apply the film to the touch screen starting at one side and smoothing it across the display. If air bubbles appear, raise the film slightly and continue smoothing the film across the display until it covers the glass surface of the display. If dust, lint or smudges are trapped between the protective film and the glass display, remove the protective film, clean the display and apply the protective film again.

Adjusting the Keypad Backlight

The keypad backlight is white can be set to On or Off. The default value is On. When set to Off, the keypad backlight does not turn on during Suspend/Restart or reboots. When set to On, the keypad backlight follows the display backlight setting. The keypad backlight turns off when the display backlight dims.

Setting Date and Time Zone

Tap **Start > Settings > Control Panel > Date/Time** icon or tap the Date/Time in the taskbar.

Set Date, Time, Time Zone, and assign a Daylight Savings location on the MX9 after a warm boot or anytime.

There is very little functional change from standard desktop PC Date/Time Properties options. Adjust the settings and tap the OK button or the Apply button to save changes to the registry. Any changes take effect immediately.

Double-tapping the time displayed in the Taskbar causes the Date/Time Properties screen to appear.

Grab Time Utility

The GrabTime utility can be configured to synchronize the time with a local server during each reboot function.

Autolaunch Time-Sync

Start > Settings > Control Panel > MX9 Options > Communication

By default, TimeSync does not automatically run on the MX9. To enable TimeSync to run automatically on the MX9 using the GrabTime utility, check this checkbox.

Synchronize with a Local Time Server

By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the **My Device > Windows** folder on the MX9 to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the **My Device > System** folder on the MX9. The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Setting Power Scheme Timers

Start > Settings > Control Panel > Power > Schemes

Change the parameter values and tap **OK** to save the changes.

User Idle

An amount of time has passed, set by the User Idle timer, and the device shuts down a minimum number of services e.g., backlights. The System Idle timer and the Suspend timer have not expired yet.

System Idle

An amount of time has passed, set by the System Idle timer, and the device shuts down a few more services e.g., display. The User Idle timer has expired and the Suspend timer has not expired yet.

Suspend

Suspend mode is entered when (1) the unit is inactive for a predetermined period of time, (2) the user taps the Power key, or (3) **Start > Suspend** is chosen. Inactivity means that internal devices that reset the power state are not active.

Battery Power Scheme

Use this option when the MX9 will be running on battery power only.

Switch state to User Idle	Default is After 3 seconds
Switch state to System Idle	Default is After 15 seconds
Switch state to Suspend	Default is After 5 minutes

AC Power Scheme

Use this option when the MX9 will be running on external power (e.g., connected to an A/C power source).

Switch state to User Idle	Default is After 2 minutes
Switch state to System Idle	Default is After 2 minutes
Switch state to Suspend	Default is After 5 minutes

The timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to “Never”, the power scheme timers never place the MX9 in User Idle, System Idle or Suspend modes (even when the MX9 is idle).

Using the Battery Power Scheme Defaults listed above, the cumulative effect results in the following:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 seconds + 3 seconds),
- And the MX9 enters Suspend after 5 minutes and 18 seconds of no activity.

Setting Speaker Volume

The speaker is located on the front of the MX9 between the Scan keys and underneath the LEDs.

Speaker volume can be adjusted to a comfortable level for the listener by using the keypad or by changing parameters in a control panel.

Using the Keypad

Note: Speaker sounds must be enabled before the following key sequences can adjust the volume.

The volume is increased or decreased one step each time the volume key sequence is pressed.

To adjust speaker volume:

- Blue+V+Up Arrow and Blue+V+Down Arrow keys on the 62-key keypad.
- Orange+Scan+Up Arrow and Orange+Scan+Down Arrow keys on either keypad.
- Press any key, except the keys you used to adjust the volume, to exit.

Volume control using a keypad key press has six volume settings that match those supported by the control panel. Volume does not “roll-over” from minimum to maximum or from maximum to minimum. Continuously holding down the up or down arrow keys does not cause an automatic repeat of the up (or down) arrow key.

Using a Control Panel

Tap **Start > Settings > Control Panel > Volume & Sounds > Volume** tab. Change the volume setting and tap **OK** to save the change.

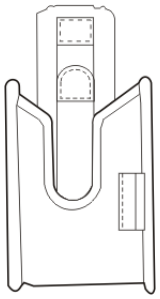
You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

As the volume scrollbar is moved between Loud and Soft, the MX9 emits a tone each time the volume increases or decreases.

Body Worn Accessories

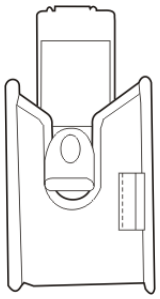
Protect the Touch Screen when using a Holster / Carrycase .

Holster without Handle



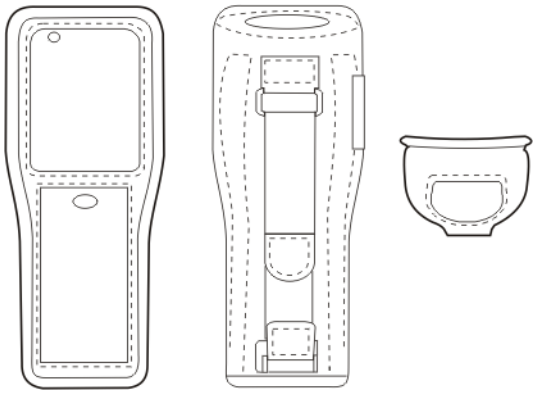
The MX9 is inserted upside-down in the holster with the touch screen facing the belt connecting the holster to the body.

Holster with Handle



The MX9 is inserted upside-down in the holster with the touch screen facing the belt connecting the holster to the body. Guide the installed trigger handle into the trigger handle notch.

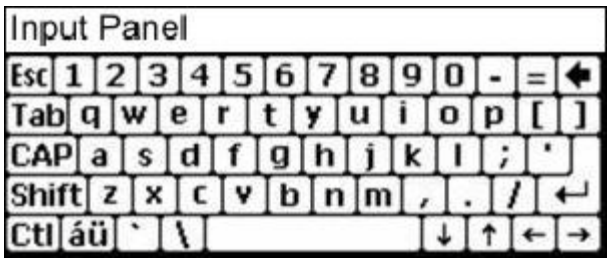
Carrycase



Remove the hand strap components from the MX9. Open the zippered case until there is enough space to insert the MX9 into the case. The touch screen must face forward so it, and the keypad, are visible through the windows in the carrycase.

Close the zippers. If desired, attach the hand strap components to the zippered case.

Using the Input Panel / Virtual Keyboard



The input panel/virtual keyboard is always available when needed e.g., text entry.

Place the cursor in the text entry field and, using the stylus:

- Tap the Shift key to type one capital letter.
- Tap the CAPS key to type all capital letters.
- Tap the áü key to access symbols.

Some applications do not automatically display the Input Panel. In this case, do the following to use the Input Panel:



Input Panel icon in the taskbar



Keyboard icon in the taskbar

1. Tap the Input Panel or Keyboard icon in the taskbar.
2. Select Keyboard from the menu.
3. Move the cursor into the text entry field when you want to enter data using the Input Panel.
4. When finished entering data, tap the icon in the Taskbar again. Select Hide Input Panel.

Connecting Bluetooth Devices

Before connecting to Bluetooth Devices:

- The system administrator has discovered, paired, connected and disconnected using EZPair (or LXEZ Pairing) control panel, Bluetooth devices for each MX9.
- The system administrator has enabled and disabled settings for the MX9.
- The system administrator has also assigned a Computer Friendly Name using EZPair control panel for the MX9.

To connect Bluetooth devices, the MX9 should be as close as possible and in direct line of sight (distances up to 32.8 feet or 10 meters) with the targeted Bluetooth device during the discovery and pairing process.

If the Bluetooth devices are in Suspend, tap the power key to wake the MX9. Using the correct procedure, wake the targeted Bluetooth device if necessary.

There may be audible or visual signals as both devices discover and pair with each other.

Bluetooth On-Screen Indicator

	MX9 is connected to one or more of the targeted Bluetooth device(s).
	MX9 is not connected to any Bluetooth device. MX9 is ready to connect with any Bluetooth device. MX9 is out of range of all paired Bluetooth device(s). Connection is inactive.

Bluetooth LED Functions

When the Bluetooth LED on the MX9 is off, Bluetooth hardware has been turned off or it does not exist in the MX9.

When the Bluetooth LED on the MX9 is on:

- the MX9 is paired with another Bluetooth device but is out of range or not connected, or
- is paired and connected to another Bluetooth device, or
- is discovering other Bluetooth devices.
- The LED blinks slowly (Bluetooth LED is on for one second, off for five seconds) when it is idle.
- The LED blinks quickly (Bluetooth LED is on for 1/4 second, off for 2 seconds when the MX9 is discovering other Bluetooth devices.
- The LED blinks normally (Bluetooth LED is on for 1/2 second, off for 1/2 second) when it is connected.

There may be audible or visual signals from paired devices as they move back into range and re-connect with the Bluetooth hardware in the MX9.

Setting Terminal Emulation Parameters

Before you make a host connection, you will, at a minimum, need to know:

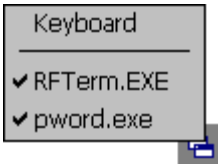
- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system to properly set up your host session.

1. Make sure the MX9 network settings are configured and functional. If you are connecting over wireless LAN (802.11*x*), make sure your MX9is communicating with the Access Point.
2. From **Start > Programs**, run RFTerm or tap the RFTerm icon on the desktop.
3. Select **Session > Configure** from the application menu and select the “host type” that you require. This will depend on the type of host system that you are going to connect to; i.e., 3270 mainframe, AS/400 5250 server or VT host.
4. Enter the “Host Address” of the host system that you wish to connect to. This may either be a DNS name or an IP address of the host system.
5. Update the telnet port number, if your host application is configured to listen on a specific port. If not, just use the default telnet port.
6. Select **OK**.
7. Select **Session > Connect** from the application menu or tap the “Connect” button on the Tool Bar. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Bar Code, etc., refer to these sections in the *RFTerm Reference Guide* for complete descriptions of these and other features.

Using the AppLock Switchpad

Note: The touch screen must be enabled..



Switchpad Menu



Switchpad Icon

Click the switchpad icon in the taskbar.

A checkmark on the switchpad menu indicates applications currently active or available for Launching by the MX9 user. When Keyboard, on the Switchpad Menu, is selected, the default input method (Input Panel, Transcriber, or custom input method) is activated.

Using the Keypad

One switch key sequence (or hotkey) is defined by the Administrator for the end-user to use when switching between locked applications. This is known as the Activation key.

When the Activation key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. MX9 key presses affect the application in focus only.

Using the Touch Screen

The figure shown above is an example and is shown only to aid in describing how the user can switch between applications using a stylus.

When the user taps the Switchpad icon with the stylus, a menu pops up listing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

Rebooting the MX9

When the Desktop/Start screen is displayed or an application begins, the power up sequence is complete. If you have previously saved your settings, they will be restored on reboot. Application panel changes are saved when OK is tapped on an application properties panel.

During the process that follows, there may be small delays while MX9 wireless clients connect to the network and Bluetooth relationships establish or re-establish.

Warmboot

A warmboot reboots the MX9 without erasing any registry data. Applications and data in RAM are preserved during a warmboot. All registry configurations are automatically preserved. Any applications stored as CAB files in the System folder and configured in the Registry to persist are reinstalled on boot up by the Launch utility.

Use the Registry control panel Warmboot button.

Restart (or Cold Boot)

The Restart (or cold boot) function reboots the device and reloads RAM. Use the Registry control panel Load Factory Defaults button to erase the registry and set the registry back to factory defaults.

Note: Because of the extreme nature of Restart, Honeywell recommends using this command only in an emergency (or when instructed to do so as part of a specific MX9 procedure).

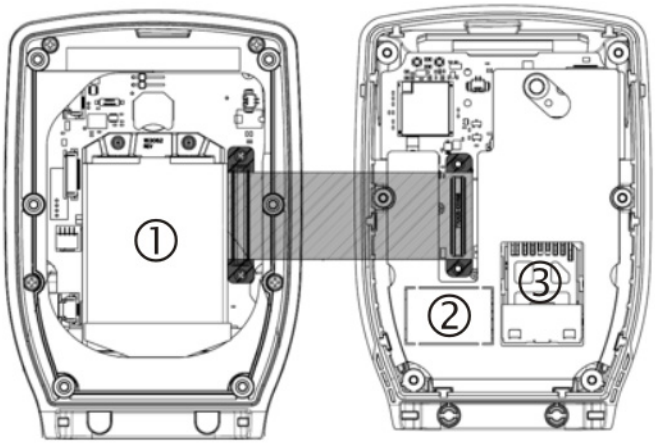
Installing the SIM Card

Tools required: standard size Phillips screwdriver (not supplied).

Note: Installing or removing accessories should be performed on a clean, well-lit surface. When necessary, protect the work surface, the MX9, and components from electrostatic discharge.

Note: Contact Technical Assistance (page 15-1) if you need help when installing or removing a SIM card.

The expansion slots in the MX9 are accessible via the hatch. The hatch can be opened using a standard size screwdriver. When the hatch is opened, the MX9 automatically shuts down. It is good practice to save any changes then perform an orderly shutdown to preserve RAM contents before opening the hatch.



1. Summit radio card located in the back half of the MX9 assembly.
2. SIM card located in the front half of the MX9 assembly.
3. SD card located in the front half of the MX9 assembly.

When the hatch is open during this procedure, do not remove any cables or allow them to kink.

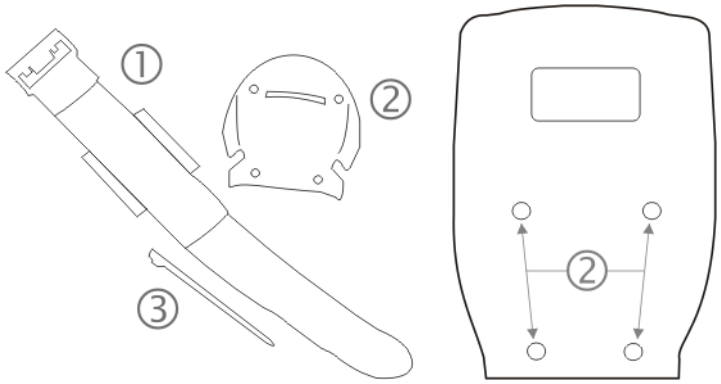
When the hatch is being closed, carefully move cables and wires back into the cavity before securing the hatch.

Before securing the hatch completely, examine the seam between the front and back half of the MX9. If the gasket is off-center, loosen the screws a little, adjust the gasket and re-tighten the screws.

Press the Power button to turn the MX9 on.

Attaching the Hand Strap

Note: Either the trigger handle is attached to the MX9 or the hand strap is attached, not both. In the absence of a trigger handle, the hand strap should be used at all times. The hand strap is pre-installed on a MX9 that is purchased without a trigger handle.

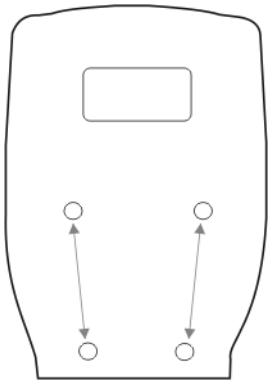


1. Place the MX9 with the screen facing down, on a flat stable surface.
2. Place the hand strap base (2) in the grooved area, matching the screw holes in the hand strap base with the screw holes in the body of the MX9.
3. Insert the screws (supplied) into each of the four holes and fasten the base securely.
4. Slide the hand strap bottom clip pins into the slots at the base of the MX9 and pull the strap towards the top of the MX9 until the top clip slips into the groove.
5. Making sure the closed loop fastener surface on the hand strap are facing up, slide the strap through the latch in the top clip.
6. Fold the end of the strap over so that the closed loop fastener surfaces mate evenly and the hand strap is secured to the MX9.
7. Test the strap's connection making sure the MX9 is securely connected to each end of the strap connectors.

Check the closed loop fastener and hand strap base connection frequently. If loose, they must be tightened or replaced before the MX9 is placed into service again.

Attaching the Trigger Handle

Pressing the trigger on the trigger handle activates the integrated scanner and functions the same as the Scan key on the keypad. With the handle installed the Scan key on the keypad remains active. The trigger duplicates the operation.



- The handle is built of a durable, flexible plastic.
- The handle will not detach from the MX9 if the unit is dropped.
- The trigger handle is a mechanical device. Battery or external A/C power is not required for operation.
- The trigger handle does not need to be removed when replacing the main battery pack.
- The trigger handle might also be called a pistol grip.

Equipment needed: Torque wrench capable of torquing to 3±1 in/lb (.34±.11 N/m).

Either the trigger handle or the hand strap is attached, not both. Honeywell recommends that, in the absence of a trigger handle, the hand strap be used at all times.

1. Place the MX9 with the screen facing down, on a flat stable surface.
2. Remove the hand strap and hand strap base, if installed.
3. Place the trigger base into the molded area on the back of the MX9.
4. Ensure that the battery can be inserted into the battery compartment before securing the trigger handle in place.
5. Attach the trigger handle to the MX9 (as shown above) with the screws provided.
6. Torque the pan head screws to 3±1 in/lb (.34±.11 N/m).
7. Secure the strap tether to the trigger handle.
8. Place the stylus in the stylus holder in the trigger handle.

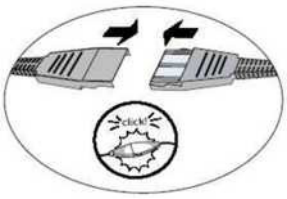
Periodically check the trigger handle for wear and the connection for tightness. If the handle gets worn or damaged, it must be replaced. If the trigger handle connection loosens, it must be tightened or replaced before the MX9 is placed in service.

Adjusting the Headset / Microphone and Securing the Cable



The headset consists of an earpiece, a microphone, a clothing clip and a cable. The headset attaches to the audio cable end of the voice cable which attaches to the MX9.

Align the audio connector and the headset quick connect cable end. Firmly push the cable ends together until they click and lock in place.



Do not twist the microphone boom when adjusting the microphone. The microphone should be adjusted to be about two finger widths from your mouth.

Make sure the microphone is pointed at your mouth. Note the small “Talk” label near the mouthpiece. Make sure the Talk label is in front of your mouth. The microphone cable can be routed over or under clothing.

Under Clothing

- Leave the cable exposed only at the top of the collar.
- Be sure to leave a small loop of cable to allow movement of your head.

Over Clothing

- Use clothing clips to hold the cable close to your body.
- Tuck the cable under the belt, but leave a small loop where it goes under the belt.
- Do not wear the cable on the front of your body. It may get in your way or get caught on protruding objects.

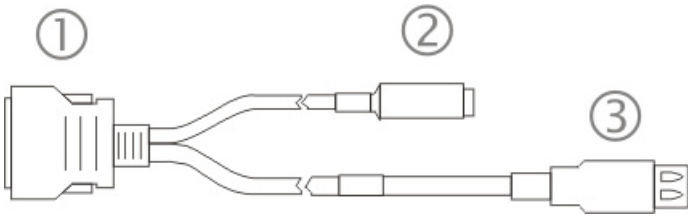
Connecting Cables to the MX9

Note: Do not connect or disconnect cables in a Hazardous location.

Connecting the USB Host and Power Cable

AC/DC Adapter must be assembled before this process begins.

Do not connect AC power to the AC Adapter until instructed in the following procedure:



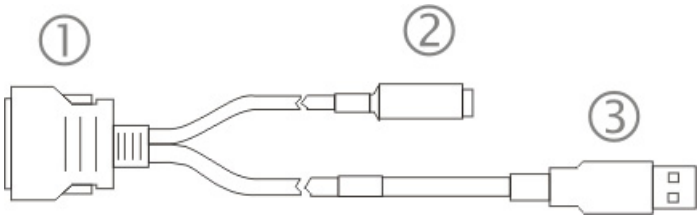
1. Holding the cable I/O connector (1), pinch the catch release buttons in until the catches are open. Connect the cable to the MX9 I/O port by matching the shape of the I/O connector on the cable with the shape of the I/O connector at the base of the MX9. Release the catch release buttons.
2. Insert the AC adapter single pin cable (2).
3. Connect the AC Adapter to a power source (wall outlet).
4. Insert the USB host plug (3) into the USB Host port.

The MX9 and the host device are connected.

Connecting the USB Client and Power Cable

AC/DC Adapter must be assembled before this process begins.

Do not connect AC power to the AC Adapter until instructed in the following procedure:



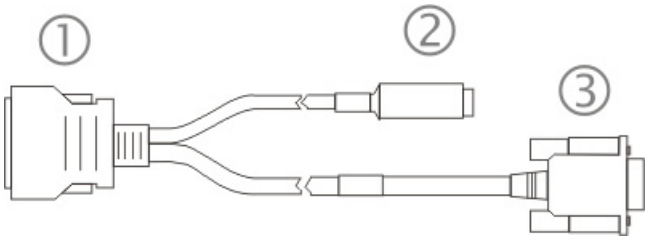
1. Holding the cable I/O connector (1), pinch the catch release buttons in until the catches are open. Connect the cable to the MX9 I/O port by matching the shape of the I/O connector on the cable with the shape of the I/O connector at the base of the MX9. Release the catch release buttons.
2. Insert the AC adapter single pin cable (2) .
3. Connect the AC Adapter to a power source (wall outlet).
4. Insert the USB client plug (3) into the target USB Client port.

The MX9 and the USB client are connected.

Connecting the Serial and Power Cable

AC/DC Adapter must be assembled before this procedure begins.

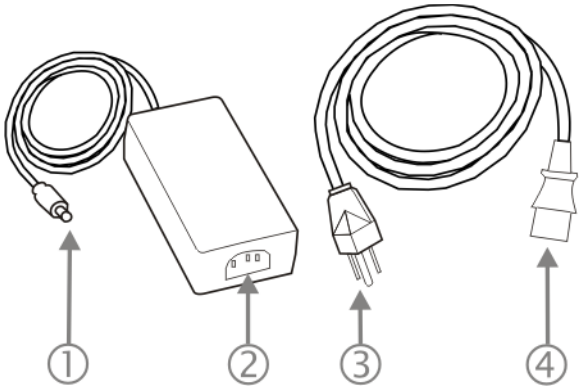
Do not connect AC power to the AC Adapter until instructed to do so in the following procedure:



1. Holding the cable I/O connector (1), squeeze the catch release buttons in until the catches are open. Connect the cable to the MX9 I/O port by matching the shape of the I/O connector on the cable with the shape of the I/O connector at the base of the MX9. Release the catch release buttons.
2. Connect the AC adapter single pin cable end (2).
3. Connect the assembled AC/DC Adapter to a power source (wall outlet).
4. Connect the RS232 cable end (3) to the desired serial device. Turn the thumbscrews clockwise until the connection is finger-tight.

The MX9 and the serial device are connected.

Connecting an External Power Supply



To apply external power to the MX9 follow the steps below in sequence.

1. Plug the 3 prong AC adapter cable end (3) of the external power assembly into an AC power source (e.g., wall outlet).
2. Firmly press the female end (4) of the power cable into the male connector (2) on the power adapter. When AC power is being supplied to the power adapter, the LED on the power adapter illuminates green.
3. Squeeze the catches of the I/O connector and push the cable connector into the MX9 I/O port until it clicks. The click means the connector is seated firmly.
4. Press the power cable connector pin (1) from the power adapter into the connector on the (USB/Power or Serial/Power) cable attached to the base of the MX9. External power is now being supplied to the MX9.

Whenever possible, use the AC power adapter with the MX9 to conserve the main battery power

Replacing the CLA Fuse

Equipment needed: 5A fuse of the same size and amperage.

1. Remove the CLA from the cigarette lighter outlet on the vehicle.
2. Disconnect the cable from the MX9.
3. Unscrew the tip of the adapter end.
4. Replace the blown fuse with a fuse of the same rating and size.
5. Screw the tip back on to the adapter end, replacing any previously removed parts in the order in which they were removed.

Upon reassembling the cigarette lighter adapter with the new fuse, and plugging it into the cigarette lighter port on the vehicle -- if the LED on the CLA does not illuminate green, there may be a problem with your vehicle power source.

Cleaning the Touch Screen and Scanner Aperture

Note: These instructions are for components made of glass. If there is a removable protective film sheet on the display, remove the film sheet before cleaning the screen.

Keep fingers and rough or sharp objects away from the bar code reader scanning aperture and the mobile device touch screen.

If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex® without vinegar or use Isopropyl Alcohol. Dampen the cloth with the cleaner and then wipe the surface.

Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the glass surface. Use a clean, damp, lint-free cloth.

Do not scrub optical surfaces. If possible, clean only those areas which are soiled. Lint and particulates can be removed with clean, filtered canned air.

Startup Help

Issue:

Can’t change the date/time or adjust the volume.

Solution:

AppLock is installed and may be running in User Mode on the MX9. AppLock user mode restricts access to the control panels.

Issue:

Touch screen is not accepting stylus taps or needs recalibration.

Solution:

Press Ctrl+Esc to force the Start Menu to appear. Use the tab, backtab and arrow keys to move the cursor from element to element. Press Enter to open folders or start a program e.g., Registry panel Warmboot button.

Issue:

MX9 seems to lockup as soon as it is rebooted.

Solution:

There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, and Bluetooth relationships establish or re-establish.

When the desktop appears or an application begins, the MX9 is ready for use.

Issue:

New MX9 main batteries don't last more than a few hours.

Solution:

New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the MX9 is always ‘on’ even when in the Suspend state and draws battery power at all times.

Issue:

Keep losing ActiveSync connection between my host computer and the MX9.

Solution:

Disconnect the USB cable from the host, wait 1-2 seconds and reconnect the cable. The MX9 should not enter Suspend as long as an ActiveSync session is running.

3 Hardware Configuration

802.11 b/g and a/b/g Wireless Client

The MX9 has an 802.11x network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is a 806 MHz Marvell PXA-320 CPU. The OS image is stored in on-board flash memory. The MX9 supports the following I/O components of the core logic:

- One serial port (DTE) with appropriate power for a WAN radio
- One serial port (DTE) for an integrated laser decoder with ring indicator (RI)
- USB 1.1 Host (capable) with power (5V @ 500mA)
- One SSP port (capable, not implemented)
- One SDIO port for I/O expansion (capable)
- One SIM port for WAN
- One serial port (DTE) for interface with GPS receiver chip
- Non-decoding imager

System Memory

The MX9 supports 128 MB on-board RAM and 128 MB on-board Flash. Operating system and boot loader software image update is supported via expansion card and remote management via radio.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID is stored in the boot flash. A second copy of the bootloader code is stored on the internal SD Flash drive, so that if a damaged bootloader is detected, it may be re-flashed correctly.

Internal SD Memory Card

The MX9 has one SD card interface for storage of operating system and program code, as well as persistent storage.

The internal SD flash card appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows interface.

Video Subsystem

The touch screen display supports QVGA and 16 bit color depth, and is readable indoors or outdoors even in direct sunlight.

The display is transflective active-matrix TFT and has an LED backlight.

A tethered stylus is included. The touch screen surface can be activated with the stylus or a gloved or bare finger.

The Cold Storage option includes a touch screen heater and a scan aperture heater to eliminate condensation. The heaters can be enabled or disabled by the user. Once enabled, the heaters will turn on whenever the ambient temperature warrants, for example, when moving into and out of freezers or refrigerated buildings.

Power Supply

The MX9 uses one of two batteries for operation. A Lithium-Ion (Li-Ion) standard battery has a 2400 mAh capacity. Low temperature Lithium-Ion (Li-Ion) batteries have a 2100 mAh capacity.

Input/Output Connector

A single external connector at the base of the MX9 provides the following signals:

- USB Host and USB Client
- RS232 with support for powering a tethered device (e.g., scanner or imager)
- Audio in and out for headset
- Power input
- Ethernet (only accessible when MX9 is secured in a cradle docking bay)

The MX9 cables are designed to be securely connected to this port. This port is also used to connect the MX9 to the docking bay connector in cradles.

A tethered protective cap is provided to cover the I/O connector when it is not in use.

Audio Support

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset accessory cable.

Bluetooth

The MX9 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains network connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to or from the MX9. However, the MX9 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX9 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user passcode.

Bluetooth device connection supported on the MX9 includes:

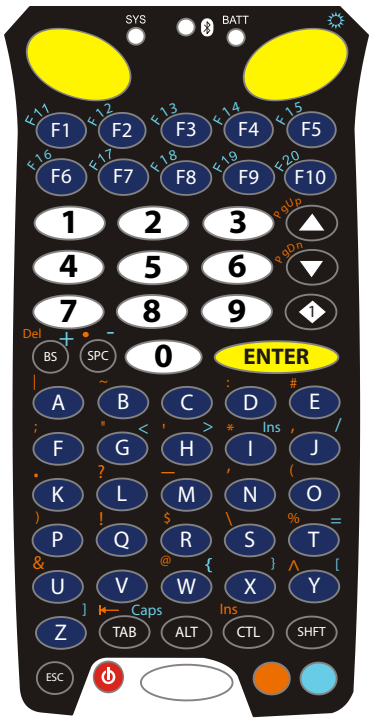
- Bluetooth scanners / imagers
- Zebra printer models
- Honeywell Back of Hand Scanner

Bluetooth devices can be paired and managed using the Bluetooth control panel.

Bar code data captured by a mobile Bluetooth scanner is manipulated by the settings in the MX9 Data Collection panel.

Multiple beeps may be heard during a bar code scan using the mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the bar code data is accepted/rejected, and other beeps from the MX9 during final bar code data manipulation.

Keypads



62-Key Keypad



38-Key Keypad

The MX9 keypad is either a 62-key full alphanumeric keypad or 38-key numeric-alpha. The 62 key keypad has an ANSI or a 5250 overlay. KeyMaps (page 11-1) are available for all keypads.

Note: The keypad backlight default setting is to follow the display backlight setting until it is changed by the user.

Modifier Keys

The orange and blue modifier keys are located at the bottom of the keypad. The Orange and Blue keys do not need to be held down while another key is pressed.

A modifier key pressed after itself toggles that modifier mode off.

A modifier keypress cancels the other modifier's active state. Then the state of the modifier key that was pressed last becomes active. For example, if the Orange modifier state is active (MX9 is currently in Orange mode), pressing the Blue key cancels Orange mode and sets Blue mode active.

Once a modifier key is pressed, the modifier map state continues until another key is pressed.

Modifier keys do not auto-repeat.

Expansion Slots

- Summit radio card
- SIMM card
- SD card

The expansion slots in the MX9 are accessible via the hatch. The hatch can be opened using a standard size screwdriver. When the hatch is opened, the MX9 automatically shuts down.

SD card configurations in 512MB, 1GB and 4GB are available from Honeywell.

Note: For best results save your changes then perform an orderly shutdown to preserve RAM contents before opening the hatch.

Power Key Functions

The Power key is located at the bottom left of the keypad. The Power On/Off key is a momentary contact. Function is as follows:

When the MX9 is in ...	Pressing the Power key ...
Off mode	boots the unit and sets it to the On mode
On mode	sets the unit in Suspend mode
Suspend mode	sets the unit in On mode
Critical Suspend mode	has no effect
Backlight off mode	sets the unit in Suspend mode

Status LEDs

Several LEDs are located on the front of the MX9 above the integrated speaker. They are:

- System Status (SYS) LED indicates power management status.
- Battery Charging Status (BATT) LED indicates main battery charging status.
- Alpha Mode Status (ALPHA) LED applies to the 38-key keypad only.
- Bluetooth Status LED applies to Bluetooth client functions.

System Status LED

Blinking Red	Battery power fail; critical suspend
Solid Red	Main battery low
Yellow / Amber	Initial few seconds when Power key is pressed

Battery Charging Status LED

Off	No battery, no AC power, battery pack not plugged in or no AC power applied
Flashing Red	Fault, battery pack fault or failure
Yellow / Amber	Standby, battery pack temperature out of range
Red	Charging, battery pack charging (icon on touch screen)
Green	Charged, battery pack fully charged. Connected to external power.

Alpha mode Status LED

Green when in alpha mode, 38-key keypad only.

Bluetooth Status LED

Blinking slowly	Bluetooth is active but not connected to a device.
Blinking medium	Bluetooth is paired and connected to a device.
Blinking fast	Bluetooth is discovering other Bluetooth devices.
Unlit	Bluetooth hardware has been turned off or does not exist in the MX9.

Scanner Status LED

The integrated scanner, and imager, Scan Status LED is centered below the MX9 keypad, next to the Power button.

- Steady green indicates a good scan
- Steady red indicates a scan is in progress
- Steady yellow/amber indicates parameter changes are being written to the integrated scanner/imager engine

The Scan Status LED illuminates when a Scan button on the MX9 is depressed (scan in progress), or the trigger on the attached handle is pressed (scan in progress), or when the scanner/imager engine parameters have been changed and the changes are being saved (writing to scan engine). While the changes are being saved, the scanner/imager is inoperable.

- The MX9 Scan Status LED does not illuminate when the Scan button is pressed on a scanner cabled to the MX9 or cabled to an MX9 cradle communication port. The Scan LED on the cabled scanner/imager illuminates.
- The MX9 Scan Status LED does not illuminate when the Scan button is pressed on a wireless Bluetooth mobile scanner paired with the MX9. The Scan LED on the wireless Bluetooth mobile scanner/imager illuminates.

Note: A scanned bar code can be accepted as a good scan or a bad scan by the MX9 bar code decoder (as configured). The appropriate audible or tactile indicator is activated.

Note: The result of the host processing (as configured) of the good scan bar code data can indicate either accept or reject. If rejected, a bad scan indicator is activated if the host process has been configured to indicate audible or tactile accept or reject.

Cold Storage

When the MX9 has been configured as a cold storage or low temperature device, it has a snowflake decal between the touch screen and the keypad.

The MX9, with its special low temperature battery and condensation controlling heaters is designed specifically for use in freezers and refrigerator environments including transitioning between the two.

Heating Elements

Heating elements activate when ambient temperature drops below 0°C (32°F). Honeywell recommends using the stylus when performing screen touch functions on the display when the temperature drops below freezing. There may be some condensation as the MX9 moves in and out of cold storage areas. The condensation on the touch screen and the scan aperture quickly dissipates.

Although no user interaction is required to enable the heating elements, the automatically controlled heating elements can be enabled and disabled using the Heaters tab in the Peripherals panel.

Vibrate Indicator

The MX9 has a vibration motor.

It is user-configurable to vibrate on a good scan, bad scan, or via an API call. The vibrations from this motor are detectable under the handstrap at the rear of non-handle units or through the trigger handle when a trigger handle is installed.

Three vibration duration settings are provided for both good and bad scan. The settings can be assigned using the Data Collection Notification control panel. The default setting for both good scan and bad scan vibration is Off.

Scanners and Imagers

Note: The maximum number of communication ports from which the Data Collection Wedge can simultaneously support input is three.

Integrated Bar Code Decoders

The MX9 may have any of the following bar code reader built in (integrated) and protected by the hatch:

- Symbol SE955 short range laser scanner engine (bar code decoding only)
- Symbol SE1524 Lorax laser scanner engine (bar code decoding only)
- Hand Held Products 5300SF laser imager engine (non-decoding)

A scan aperture heater is implemented for low temperature environments.

Tethered Bar Code Decoders

The external serial port at the base of the MX9 is used to connect (via serial tether) tethered laser scanners as needed.

Bluetooth Client Bar Code Decoders

The Bluetooth Module in the MX9 can accept data from paired Bluetooth bar code readers.

GPS Module

The MX9 default setting for GPS is Off.

GPS (Global Positioning System) is a U.S. space-based radio navigation system that provides reliable positioning, navigation, and timing services on a continuous basis. The primary function of the embedded GPS module is to provide worldwide location to applications which are running on the MX9.

GPS presence is displayed on the Peripherals control panel. Using the GPS tab, GPS power can be toggled on or off only when a GPS is installed.

4

Power Modes and Batteries

Power Modes

On

When in the On state, the display (touch screen) is on. The keyboard, touch screen and all peripherals function normally. The display backlight is on until the User Idle timer expires. The display does not turn off until the System Idle timer expires.

Only interrupts classified as User Activity events will keep the unit in the On state.

MX9 User Activity Events are:

Note: These items are not configurable selections.

- Any key on the keypad except the Power key
- Incoming data through scanner port
- Touch screen tap
- Trigger pull

The user is presented with a Power applet in the Control Panel. One tab in the applet, Schemes, is designated for the power management timeouts. This tab displays three transition states, User Idle, System Idle and Suspend.

Additionally, the OS provides a Backlight tab on the Display control panel. The Backlight tab allows the user to select the same timeout ranges provided by the User Idle scheme timers. Any changes on the **Display > Backlight** tab will also change the **Power > Schemes > User Idle** timer, and vice-versa.

The backlight for the keypad (if enabled) will always follow the display backlight.

User Idle

When transitioning from the On power state to the User Idle power state, the keypad backlight (if enabled) is dimmed and the display backlight is dimmed. User Activity Events listed below will transition the system back to the On state.

User Idle timers are set using **Start > Settings > Control Panel > Power > Schemes** tab.

Only interrupts classified as System Activity events will keep the MX9 awake in this state until a deliberate user action to put the unit into Suspend or power Off occurs. An event must be specifically coded to wake up from this state.

The following User Activity events DO transition the unit from the User Idle state to On state:

Note: These items are not configurable selections

- Any key on the keypad except the Power key
- Incoming data through the scanner port
- Touch screen tap
- Unit docked in powered cradle
- Trigger pull
- Incoming Bluetooth connection or data on the virtual COM port
- Connection of USB Device to host port

Note: The scanner port is defined as a software (SW) port. Any hardware (HW) device that sends data to the software (SW) defined scanner port will transition the unit from User Idle to On.

The following events DO NOT wake the unit from the User Idle state or reset the timers:

- COM1 CTS
- Serial connection
- USB client connection to a host PC
- Power key press (transitions to Suspend)

Example: Bluetooth Voice will not transition the unit from User Idle to On. Bluetooth Scan data will transition the unit to On as it sends the data to the scanner port.

System Idle

After transitioning to the User Idle power state, the timer is started for the transition to System Idle. When this timer expires without any further user activity, the keypad backlight (if enabled) is turned off and the display is turned off. Only interrupts classified as System Activity events will wake the unit from System Idle to User Idle. Any activity classified as User Activity will transition from System Idle to On.

System Idle timers are set using **Start > Settings > Control Panel > Power > Schemes** tab.

The following System Activity events DO transition theMX9 from the System Idle state to User Idle state:

Note: These items are not configurable selections.

- RF Data
- Ethernet Data
- Serial Data
- USB Data

Note: Pressing and releasing the Power key while the MX9 is in the System Idle state will cause it to transition to the Suspend state.

- External power applied
- Real-Time Clock (RTC)(Win32 API call CeRunAppAtTime will not work if this is turned off)
- Detection of external microphone

Wake Up Event Default Settings

Enabled	**Disabled**
Power key	Bluetooth connection
Touch screen tap	COMM CTS
Integrated keypad key press	Internal serial port device IRQ
USB client connection	Push to talk on audio headset
External power applied	Detection of external microphone
Real-time clock	
Trigger handle trigger press	

Events that do NOT wake up from Suspend - these events are not available to be configured to wake the unit up from suspend

- External keyboard/mouse
- Ethernet (data or connection)
- USB Host (data or connection)
- USB client disconnection
- Serial data
- Internal Serial port handshaking (WAN, etc)
- 802.11 radio
- Docked signal (i.e., a non-powered cradle would not wake the MX9 up, but a powered cradle could be a wake up event if External Power is set to be a wake up event)
- MPF (Main Power Failure)
- Audio data
- Display data

Critical Suspend

The purpose of the Critical Suspend mode is to maintain data stored in RAM with minimum power consumption. If the Main Battery is removed, the Backup Battery is supplying power to the MX9 during Critical Suspend Mode. If Main Battery power is re-applied, the device will transition to Suspend mode. If Main Battery power is not made available before the Backup Battery is depleted, the unit enters Off Mode.

Off

The MX9 enters the Off Mode when the Main Battery and the Backup Battery are depleted or when Shutdown is selected from the Start menu.

Batteries

The MX9 is designed to work with a replaceable 2400 mAh Lithium-Ion (Li-Ion) battery pack from Honeywell. Under normal conditions it should last approximately eight hours before requiring a recharge.

MX9 low temperature 2100 mAh Lithium-Ion (Li-Ion) batteries (designed for freezer environments and with a blue label) have an average use time of 4 hours before requiring a recharge.

During very heavy scanning or wireless transmitter use, the operating time of the battery may be less.

HazLoc versions of the MX9 require a screwdriver to remove the plate covering the battery release mechanism.

When the MX9 is docked in a powered cradle, the battery in the MX9 is recharged through the cradle connector in the docking bay. An extra Li-Ion battery pack can be recharged in a powered desktop cradle. The battery is fully recharged in a powered cradle in less than 4 hours. The MX9 can be Off, in use or in Suspend Mode while the battery is recharging.

Note: New main battery packs must be charged prior to use. This process takes up to four hours in an MX9 Battery Charger and six hours when the MX9 is connected to external power.

Checking Battery Status

Open the Battery control panel. Battery voltage level, status and power remaining is displayed.

Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the MX9 Multi-Charger or the MX9 unit.

When the main battery pack is properly installed in the unit it provides up to eight hours of operation depending upon use and accessories installed. The battery pack is resistant to impact damage and falls of up to four feet to a concrete surface. Under normal conditions it should last approximately eight hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

When the MX9 is docked in a powered cradle, the battery in the MX9 is recharged through the cradle connector in the docking bay. An extra Li-Ion battery pack can be recharged in a powered desktop cradle. The battery is fully recharged in a powered cradle in less than 4 hours. The MX9 can be Off, in use or in Suspend Mode while the battery is recharging.

Note: When the main battery and internal battery are fully depleted, the MX9 turns off. The operating system reverts to the last saved registry settings when a fully powered battery is inserted and the MX9 is turned on.

Battery Hotswapping

Important: When the internal battery power is Low or Very Low connect the AC adapter to the MX9 before replacing the main battery pack.

When the main battery power level is low, the MX9 will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the MX9 using an AC Adapter.

You can replace the main battery by first placing the MX9 in Suspend Mode then removing the discharged main battery and installing a charged main battery within a five minute time limit (or before the Super-cap internal battery depletes). When the main battery is removed the MX9 enters Critical Suspend state; the MX9 remains in Suspend mode, the display is turned off and the internal battery continues to power the unit for at least five minutes.

Though data is retained, the MX9 cannot be used until a charged main battery is installed. After installing the new battery, press the Power key. Full operational recovery from Suspend can take several seconds while the client is reestablishing a network link. If the internal battery depletes before a fully charged main battery can be inserted, the MX9 will turn Off.

Low Battery Warning

It is recommended that the main battery pack be removed and replaced when its energy depletes. When the main battery Low Battery Warning appears (the Status LED remains a steady red) perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be saved.

Super-cap Internal Battery

The MX9 has an internal battery that is designed to provide limited-duration electrical power in the event of main battery failure. The energy needed to maintain the internal battery near full charge at all times is drawn from the MX9 main battery. It takes 5 minutes or less to fully charge the internal battery. The duration of internal battery life is dependent upon operation of the MX9, its features and any operating applications. The internal battery has a minimum service life of two years. The Super-cap internal battery is replaced by Honeywell.

Handling Batteries Safely

- Never dispose of a battery in a fire. This may cause an explosion.
- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.

Caution

Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.

NiMH and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

External Power Supplies

External power supplies are available for the following:

- any I/O cable with a power connector
- desk cradle
- vehicle cradle
- car power adapter (CLA)
- Battery Charger

The indoor power supplies (e.g., AC/DC Adapters) use IEC320-C 14 AC power connectors.

The car power adapter uses the cigarette lighter adapter (CLA) and is powered by the vehicle's automotive 12V battery. The adapter power supply converts the input voltage into a voltage suitable to power the MX9 and charge the unit's internal backup battery.

The vehicle mount cradle uses a 36V, 24-60V or 70-150V DC-DC power supply.

Note: The MX9, desk cradle and battery charger use the same external power supply.

AC/DC 15V Power Supply

The MX9 receives AC/DC power from the AC/DC (15 VDC - 4 Amp - 60 Watt) Power Supply. The MX9 external power connection is part of the serial cable assembly and the USB cable assembly.

The AC/DC Power Supply is connected to a wall outlet then to the power cable secured to the base of the MX9.

Note: The Honeywell-approved AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

The indoor power supply has a IEC320-C 14 AC power connector.

When the power supply is receiving AC/DC power from the wall outlet, an LED on the power supply illuminates green. The green LED indicates the power supply is ready for use.

This AC/DC power supply is designated for:

- the MX9 I/O port multi-cables
- the MX9 desktop cradle
- the MX9 battery Charger

There are specific DC/DC power supply adapters for the MX9 vehicle cradle; do not use any other power supply with the vehicle cradle.

Car Power Adapter

The MX9 Car Power Adapter is a self-contained unit. The cable has one and a half feet of coiled cord and one and a half feet of straight cord. The coiled portion is on the end of the adapter. An LED on the adapter illuminates when the car power adapter is receiving vehicle input power.

The cigarette lighter adapter contains a power supply which converts the vehicle’s nominal 12V to 15V, a voltage suitable to power the MX9 and charge the MX9 battery.

One end consists of a plug compatible with a standard vehicle cigarette lighter adapter (CLA). The Car Power Adapter has a standard size CLA plug that uses center positive (+12V) and sleeve ground. A replaceable fuse is provided on the input side.

The other end of the three foot cable connects to the MX9 36-pin I/O port. It has a security latch for stability when the MX9 is connected to the Car Power Adapter cable.

5 Software Configuration

Introduction

There are several different aspects to the setup, configuration and operation of the MX9. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this section are to be used as examples only, the configuration of your specific MX9 computer may vary. The following sections provide a general reference for the configuration of the MX9 and some of its optional features.

Operating System

The MX9 operating system and revision level is displayed on the Desktop. This is the default setting for the Windows CE Desktop Display Background.

Windows CE Operating System

Note: For general use instruction, refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the MX9.

This chapter assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers. Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX9 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the MX9 keyboard. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	**To …**
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

Shift and Ctrl keys can be used with the touch screen for multiple selection of items as well. To select disconnected items, press the Ctrl key and then touch the screen for the items to be selected. Press the Ctrl key again to terminate this mode. To select a contiguous set of items, press the Shift key, then touch the first item in the series and the last item in the series. Press the Shift key again to terminate the selection mode.

The touch screen provides equivalent functionality to a mouse:

- A touch on the touch screen is equivalent to a left mouse click. A touch and hold is equivalent to a right mouse click.
- Many items can be moved by the "drag and drop" method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double click.

Warmboot

A warmboot reboots the MX9 without erasing any registry data. Configuration settings and data in RAM are preserved during a warmboot. Network sessions are lost and any data in running applications that has not been previously saved may be lost. CAB files already installed remain installed.

There are several warmboot methods available:

- Using the Registry control panel tap the Warmboot button. The MX9 immediately warmboots.
- Using the Start menu, select **Start > Run** and type WARMBOOT in the text box. Press Enter. The MX9 immediately warmboots. The WARMBOOT text command is not case-sensitive. The text typed in the text box can be upper or lower case or a combination of upper and lower case letters.
- Using the keypad, press the Ctl key and release it, press the Alt key and release it, press the Del key combination and release it. The MX9 immediately warmboots.

Clearing Persistent Storage / Reset to Default Settings

Use the Registry control panel Restart button to set the MX9 registry back to factory defaults. No other clearing is available or necessary.

Folders Copied at Startup

The following folders are created in the System folder, they are copied at startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs
AppMgr	copied to	Windows\AppMgr
Recent	copied to	Windows\Recent

This function copies only the folder contents, no sub-folders.

The Windows\Startup folder is not copied on startup because copying this folder has no effect on the system or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by Launch.

Saving Changes to the Registry

The MX9 saves the registry when you:

- Tap **Start > Run** then type Warmboot. Tap **OK**.
- Perform a Suspend / Resume function (by pressing the Pwr key and then pressing it again).

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g., 0 seconds).

The registry is automatically saved every 10 seconds if anything has changed. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g., Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

Software Load

The software loaded on the MX9 consists of Microsoft® Windows® CE 5 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Microsoft® Windows® CE 5 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Optional)

Note: Contact Technical Assistance for software updates and CAB files as they are released.

Software Applications

The following applications are included:

- WordPad
- Data Collection Wedge (bar code result manipulation)
- ActiveSync
- Transcriber
- Internet Explorer

Bluetooth (Optional)

Only installed on a Bluetooth equipped MX9. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX9. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each MX9.

The Bluetooth control panel can also be accessed by double tapping the Bluetooth icon in the taskbar or on the desktop.

RFTerm (Optional)

RFTerm is installed by Honeywell when ordered. The application can also be accessed by double tapping the RFTerm desktop icon or by running the RFTerm application in the Programs folder.

Avalanche

The Wavelink Avalanche Enabler installation file is loaded on the MX9 by Honeywell; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. Following installation, the Wavelink Avalanche Enabler will be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Software Development

The *CE API Programming Guide* documents unique API calls for the MX9. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found the Technical Support Portal. Contact Technical Assistance for more information.

Accessing Files on the SD/CF Card

Tap the My Device icon on the Desktop then tap the System icon.

A SD/CF card is used for permanent storage of the MX9 drivers, CAB files and utilities. It is also used for registry content back up. CAB files, when executed, are not deleted.

Always perform a warm reset (Start / Run / Warmboot) when exchanging one card for another.

Utilities

The following files are pre-loaded.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key:

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

Note: All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a Compact Flash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then 3 mandatory values are added:

FileName is the name of the CAB file, with the path (usually \System).

Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file.

FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

1. Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.

2. Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

3. PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for FileName to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.
- If the Installed flag is set, auto-launch looks for the FileCheck file. If it is present, the CAB file is installed, and that registry entry is complete. If the FileCheck file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.
- To force execution every time (for example, for AUTOEXEC.BAT), use a FileCheck of “dummy”, which will never be found, forcing the item to execute.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch will continue, leaving the loading process to run independently. For other persist keys (including .CAB files), Launch will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Note: Registry entries may vary depending on software revision level and options.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the System folder, Launch automatically copies all of the files in these directories to the respective folder on the SD/CF drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

*Note: Files in the Startup folder are executed, but only from **System > Startup**. They are not copied to another folder.*

REGEDIT.EXE

Registry Editor – Use caution when editing the Registry and make a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g., REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

Note: The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the event of a restart, copy the file to the System folder on the MX9 or store a copy of the REG.TXT file on a PC.

WARMBOOT.EXE

Double tap this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double tapping a sound file (e.g., WAV) causes WavPlay to open the file and run it in the background.

MX9 Command-line Utilities

Command line utilities can be executed by **Start > Run >** *[program name].*

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap **Start > Run** and type **prtscrn** and tap **OK**, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and the screen captured file (*scrnnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Desktop

Note: For general use instruction, refer to commercially available Windows CE user's guides or the Windows on-line Help application installed in the mobile device.

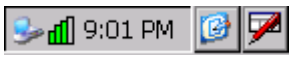
The MX9 Desktop appearance is similar to that of a desktop PC running Windows XP or later. At the bottom of the screen is the Start button. Tapping the Start Button causes the Start menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

Desktop Icons

At a minimum, the desktop displays icons for My Device, Internet Explorer and the Recycle Bin. Following are a few of the other icons that may be on the MX9 Desktop. Contact Technical Assistance (page 15-1) for the latest updates and upgrades for your operating system.

Icon	Function
	My Device. Access files and programs.
	Recycle Bin. Storage for files that are to be deleted.
	Bluetooth shortcut. Discover and then pair with nearby discoverable Bluetooth devices.
	My Documents shortcut. Storage for downloaded files / applications.
	Internet Explorer shortcut. Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from Honeywell).
	SCU shortcut. Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
	Wavelink Avalanche eXpress Scan shortcut. This utility allows an administrator to scan bar codes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the windows device. eXpress Scan uses bar codes created with eXpress Config.
	RFTerm shortcut. RFTerm is an optional terminal emulation program for Honeywell devices with a Windows operating System. When RFTerm is installed, this icon is displayed on the desktop.
	A shortcut to the Remote Desktop Connection utility.
	Avalanche shortcut. Wavelink Avalanche Mobility Center (Avalanche MC) is a remote client management system that is designed to distribute software and configuration updates to monitored devices, including computers with Microsoft Windows CE. The enabler for Wavelink Avalanche is loaded on the device but not installed. When the enabler is installed this icon is displayed on the desktop.
	Shortcut to the demo version of Wavelink Telnet CE. Contact Technical Assistance for licensing information. When installed, license details are maintained in the Wavelink tab in the License Viewer control panel.
	Start button. Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar



The number and type of icons displayed are based on the device type, installed options and MX9 configuration.

My Device Folders

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal Flash Card (CAB file storage)	Yes
Storage Card or SD Card	Additional optional storage space	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Wavelink Avalanche Enabler (Optional)

Note: If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

Related Manual: *Using Wavelink Avalanche on Windows Computers*

The MX9 has the Avalanche Enabler installation files loaded but not installed when it is shipped. The installation files are located in the System folder. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the *Avalanche Update Settings* panel through the *Enabler Interface*.

Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the “?” button to access Internet Explorer Help.

Start Menu Program Options

The following list represents the factory default program installation. Your system may contain different items from those shown below, based on the software and hardware options purchased.

Program		Function
Communication		Stores Network communication options
	ActiveSync	Transfer files between the MX9 and a host computer
	Connect	Run this command after setting up a connection
	Start (or Stop) FTP Server	Begin / end connection to FTP server
Command Prompt		The command line interface in a separate window
eXpress Scan		Option. Requires Wavelink Avalanche option eXpress Config.
Internet Explorer		Access web pages on the world wide Internet
Microsoft WordPad		Opens an ASCII notepad
Remote Desktop Connection		Log on to a Windows Terminal Server
RFTerm		Option. Terminal emulation application.
Settings		Access to all Control Panels, a shortcut to the Network and Dialup Control Panel and access to Taskbar options.
Summit		Set Summit radio / network parameters
Transcriber		Enter data using the stylus on the touch screen
Wavelink Avalanche		Option. Remote management for networked devices
Windows Explorer		File management program

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.

Communication

Start > Programs > Communication

ActiveSync

ActiveSync is pre-loaded. Using Microsoft ActiveSync you can copy files from your MX9 to a host computer, and vice versa. Once an ActiveSync relationship (partnership) has been established with Connect (on a host computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the MX9.

Connect and HSM Connect (or LXEConnect)

Upon cabling your MX9 to a host computer, and ActiveSync on the host computer opens, if the Connect or HSM Connect (or LXEConnect) application does not open on your MX9, contact Technical Assistance (page 15-1).

Start FTP Server / Stop FTP Server

Start > Programs > Communication > Start (or **Stop**) **FTP Server**

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Summit

Start > Settings > Control Panel > Summit

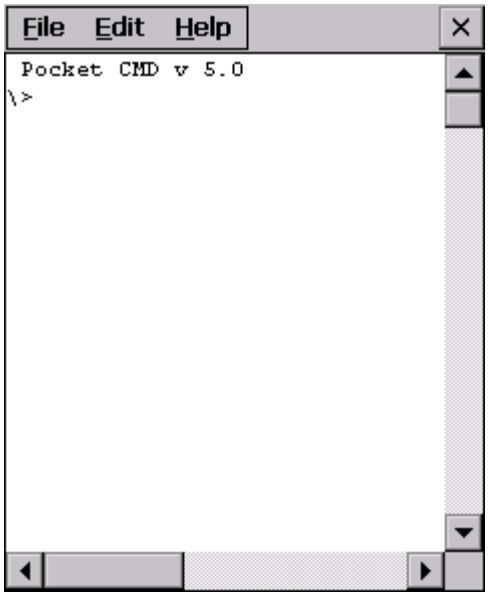
Use this option to set up radio client profiles. The Summit Control Panel can also be accessed by doubletapping the Summit icon in the taskbar or on the desktop.

Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Command Prompt

Start > Programs > Command Prompt



Type **help cmd** at the command prompt to view valid Pocket PC (Console) commands. Exit the command prompt by typing **exit** at the command prompt or tap **File > Close**.

eXpress Scan

The eXpress Scan utility allows an administrator to scan bar codes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the MX9. eXpress Scan uses bar codes created with eXpress Config.

Internet Explorer

Start > Programs > Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the **?** button to access Internet Explorer Help.

Microsoft WordPad

Start > Programs > Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad. By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g., .RTF or .DOC. Tap the **?** button to access WordPad Help.

Remote Desktop Connection

Start > Programs > Remote Desktop

There are few changes in the Windows CE version of Remote Desktop as it relates to the general desktop Windows PC Microsoft Remote Desktop options.

If installed, Remote Desktop on the MX9 can be accessed by *Start > Programs > Remote Desktop*.

Select a computer from the drop down list or enter a host name and tap the Connect button.

Tap the **Options >>** button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the **?** button to access Remote Desktop Connection Help.

Settings

Start > Settings

The Settings menu option may include the following:

Control Panel	All control panels
Network	Shortcut to the *Network and Dialup Connections* control panel. Connect to a network, create a new connection, and adjust parameters for client connections.
Taskbar	Set Taskbar parameters

Transcriber

Start > Settings > Control Panel > Input

1. To make changes to the Transcriber application, tap the keyboard icon in the status bar.
2. Select Transcriber from the pop-up menu.
3. Open the Input control panel and tap the Options button. Transcriber Options (Start > Settings > Control Panel > Input Panel) are available only when Transcriber is selected as the active input method.

Tap the **?** button or the Help button to access Transcriber Help.

Windows Explorer

Start > Programs > Windows Explorer

There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the **?** button to access Windows Explorer Help.

Taskbar

Start > Settings > Taskbar

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

When the taskbar is auto hidden, press the Ctrl key then the Esc key to make the Start button appear.

Tapping the Taskbar option on the Settings menu displays the Taskbar General tab and the Taskbar Advanced tab.

See Taskbar Icons (page 5-12).

General Tab

Setting	Default
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled



Advanced Tab



Expand Control Panel

Tap the check box to have the Control Panel folders appear in drop down menu format from the **Settings > Control Panel** menu option.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

Taskbar Icons

As MX9 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start > Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the MX9 and Honeywell unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

Icon	Function
	Wireless Zero Config - Inactive / Connected / Not Connected. Tapping the icon opens the Wireless Zero Config utility.
	Bluetooth - Connected / Disconnected. Tapping the icon opens the Bluetooth control panel.
	ActiveSync Connection.
	Cerdisp connected (displayed when HSM Connect (or LXEConnect) is connected).
	Summit Client signal indicator - No signal / Excellent signal. Tapping on the icon opens the Summit Client Utility.
	Battery charge indicator. Percent of battery charge is indicated.
	External power connected
	Current time. Tapping the time display opens the Date/Time control panel.
	Tap this icon to return to the Desktop.
	AppLock switchpad.
	Input method - Keyboard / Input panel / Transcriber.
	CapsLock active.
	No modifier key is in focus.
	Orange modifier key active.
	Blue modifier key active.
	Shift modifier key active.
	Multiple modifier keys active - Shift plus Orange.

Upgrading the Operating System

Introduction

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes.

The OS upgrade files are unique to your MX9 physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

Updates and Language Options

Same Language to Same Language

During the upgrade process all settings revert to factory defaults. Parameters will need to be changed from factory defaults to your preferred values at the conclusion of the upgrade process.

Change Language during Upgrade Process

When changing from one language to another during the upgrade process, all files in the System folder will be deleted as the system is re-partitioned and all system settings are cleared. Parameters will need to be changed from factory defaults to your preferred values at the conclusion of the upgrade process.

Preparation

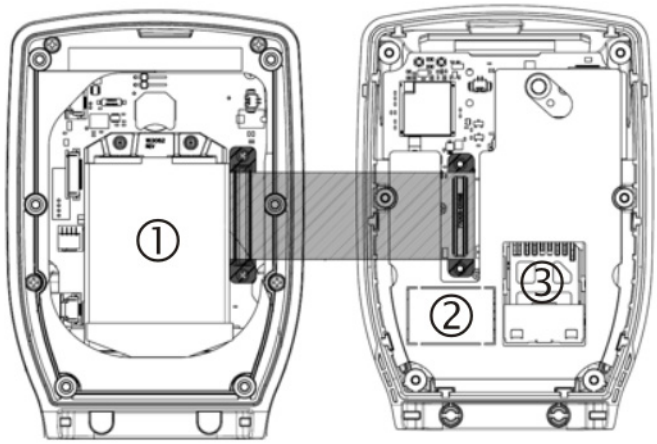
- Contact Technical Assistance to get the OS upgrade files from Honeywell.
- Put the upgrade files on a PC with ActiveSync capability.
- Copy the upgrade files from the PC to a SD card.
- Use ActiveSync to backup MX9 user files and store them elsewhere before beginning an upgrade on the MX9.
- Always perform MX9 updates when it has a fully charged main battery and/or a dependable external power source connected to the MX9.
- Removing or installing the SD card should be performed on a clean, well-lit surface.

Accessing the SD Card Slot

Tools required: standard size Phillips screwdriver (not supplied by Honeywell).

The expansion slots in the MX9 are accessible via the hatch. The hatch can be opened using a standard size screwdriver. When the hatch is opened, the MX9 automatically shuts down. It is good practice to save any changes then perform an orderly shutdown to preserve RAM contents before opening the hatch.

When the hatch is open during this procedure, do not remove any cables or allow them to kink.



1. Summit radio card located in the back half of the MX9 assembly.
2. SIMM card located in the front half of the MX9 assembly.
3. **SD card** located in the front half of the MX9 assembly.

Procedure

While the hatch is open slide the installed SD card out of the slot. The MX9 may not have a SD card in the slot because the OS is in flash.

1. Place the card with the new image files on it into the SD slot. The label on the SD card should be facing up.
2. Close the hatch. When the hatch is being closed, carefully move cables and wires back into the cavity before securing the hatch. Before securing the hatch completely, examine the seam between the front and back half of the MX9. If the gasket is off-center, loosen the screws a little, adjust the gasket and re-tighten the screws.
3. Press the Power button to turn the MX9 on.
4. The update run file in **My Device > Storage Card** automatically launches.
5. Important: If a failure occurs during the update, DO NOT RESTART (or coldboot). Follow the instructions on the screen to Exit the update utility then restart the update utility.
6. Do not touch the device until the install/update is complete.
7. When the process is finished, remove the SD card following the instructions in Accessing the SD Card Slot.
8. When finished, press the Power button.

Check the OS update version by viewing the **About** or **About Info** (or About LXE) panels.

Note: If the application displays "Update OS Image Failed" or "Update Boot Loader Image Failed", do not Restart the system manually. Perform a warm boot, then try the upgrade again. Restarting will cause a system crash, since there is no valid image in the MX9 system.

Upgrade Help

Issue:

The powered device won't boot up after the upgrade is finished.

Solution:

Contact Technical Assistance (page 15-1) if the device won't boot up after the upgrade is finished for re-imaging options.

Warning: Opening the device e.g., removing endcaps or access panels, etc. could void the user's authority to operate this equipment.

Battery State and OS Upgrade

A fully charged main battery must be installed in the MX9 prior to upgrading the operating system. A prompt may appear when the battery reaches Critical Low that informs the user there is not enough power in the main battery to perform the upgrade.

The operating system will not be able to execute the OS update when the battery level is too low (25% or less), as there is a high risk that the power remaining in the battery expires when executing the upgrade and the MX9 will be left in an inoperable state.

When main battery power level is too low, connect external power to the MX9 before performing the upgrade procedure. Do not disconnect external power before the process is complete.

Control Panel

Start > Settings > Control Panel or **My Device > Control Panel** link

Note: Change the language displayed on the touch screen by choosing Start > Settings > Control Panel > Keyboard and then the Key map drop down list.

Tap the **?** button for Help when changing Control Panel options.

Option	Function
About (page 5-17)	Software, hardware, versions and network IP. No user intervention allowed. Integrated scanner type is identified.
Accessibility (page 5-18)	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	AppLock Administration utility. See AppLock (page 6-1).
Battery (page 5-19)	View voltage and status of the main and backup batteries.
Bluetooth EZ Pair	Set the parameters for Bluetooth device connections. See Bluetooth Configuration (page 7-1).
Certificates (page 5-20)	Manage digital certificates used for secure communication.
Data Collection (Wedge)	Wedge utility for data collected from bar code scans. Set data collection device, notifications, data stripping, prefix/suffix, and vibration (if installed) options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign collected data manipulation parameters. See Data Collection Wedge (page 8-1).
Date / Time (page 5-21)	Set Date, Time, Time Zone, and Daylight Savings.
Device Management (page 5-22)	Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.
Dialing (page 5-22)	Connection setup for modem attached to COM port or Compact Flash slot.
Display (page 5-23)	Set background graphic and scheme. Set touch screen and keypad backlight properties and timers.
Input Panel (page 5-26)	Select the current key / data input method. Select custom key maps.
Internet Options (page 5-27)	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard (page 5-30)	Select a Key Map (or font). Set key repeat delay and key repeat rate.
KeyMap (page 5-31)	Configure KeyMap keys, RunCmd and LaunchApp.
License Viewer (page 5-36)	Displays license information for installed licensed applications.
Mixer (page 5-37)	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse (page 5-38)	Set the double-tap sensitivity for stylus taps on the touch screen.
MX9 Options (page 5-39)	Set various MX9 specific configuration options.
Network and Dialup Options (page 5-42)	Set network driver properties and network access properties.
Network Capture (page 5-43)	Monitor and capture network activity.
Owner (page 5-46)	Set the MX9 owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password (page 5-48)	Set OS access password properties for signon and/or screen saver.
PC Connection (page 5-49)	Control the connection between the MX9 and a local desktop or laptop computer.
Peripherals (page 5-50)	Enable or disable touch screen heater and scanner window heater, if installed. Set the flashlight off timer if the flashlight is installed. Use the GPS panel to toggle the GPS receiver on and off.
Power (page 5-52)	Set Power scheme properties. Review device status and properties.

Option	Function
Regional and Language Settings (page 5-54)	Set appearance of numbers, currency, time and date based on country region and language settings.
Registry (page 5-56)	Load User Defaults, Save User Defaults, Load Factory Defaults, and Warmboot.
Remove Programs (page 5-57)	Select to remove user installed programs in their entirety.
Stylus (page 5-58)	Set double-tap sensitivity properties and/or calibrate the touch panel.
System (page 5-59)	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses (page 5-62)	Select a server client license from a drop down list.
Volume and Sounds (page 5-63)	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
Wi-Fi (page 5-64)	Set the parameters for the MX9 Summit client.
WWAN (page 5-64)	Set parameters for the Wireless Wide Area Network client, if installed.

About

Start > Settings > Control Panel > About

The data cannot be edited by the MX9 user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates localized version.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	Revision level of software modules and .NET Compact Framework Version. Utilities, Drivers, Image, API, and Internet Explorer.
Network IP	Current network connection IP and MAC address. Only the first 2 adapters are shown (usually radio and ActiveSync). Bluetooth MAC address is shown (if installed).

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. For best results use caution when editing the Registry and make a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window .

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Languages

The Software tab displays any languages built into the OS image. The languages built into the OS image are noted in the Language section of this tab:

- English only – No additional languages are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian languages are ordered separately and built-in to the OS image. Built-in languages are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian languages are available in the (English only) default (extended) fonts.

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software is included in this list and the list varies depending on the applications loaded on the MX9. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

The Network IP tab displays the MAC address of the network card.

Accessibility

Start > Settings > Control Panel > Accessibility

Customize the way the MX9 keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general Windows desktop Accessibility options.

Note: The keypad StickyKeys and StickyKeys Settings on the Keyboard panel are disabled as this setting, when enabled, interferes with Honeywell's assigned sticky key implementation.

The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selected, note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.



Tab	Contents
Keyboard	Sticky Keys - Disabled. ToggleKeys - Disabled by default. Tap the Use ToggleKeys check box to enable this option. Tap the Settings button to view or change parameters.
Sound	SoundSentry is disabled by default. Tap the Use SoundSentry check box to enable this option. Tap the Settings button to view or change parameters.
Display	High Contrast is disabled by default. Tap the Use High Contrast check box to enable this option. Tap the Settings button to view or change parameters.
Mouse	MouseKeys is disabled by default. Tap the Use MouseKeys check box to enable this option. Tap the Settings button to view or change parameters.
General	Automatic reset is disabled by default. Tap the Turn off accessibility features check box to enable this option and use the drop down option to assign a timer. Notification is enabled by default. Sounds are emitted when turning a feature on or off.

Battery

Start > Settings > Control Panel > Battery

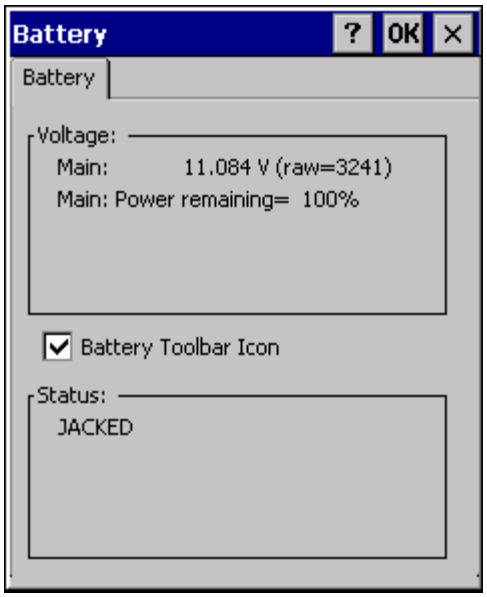
This panel is used to view the status and percentage of power remaining in the MX9 main battery. The data cannot be edited by the user.



The battery gas gauge icon resides in the system tray and shows four levels of charge – 100%, 75%, 50%, 25%. At a point below 50%, the MX9 system status LED will turn yellow and the gas gauge icon will turn yellow. At a point below 25%, the system status LED will turn red and the gas gauge icon will turn red indicating the battery is low.

Jacked is shown in the Status box when the Main battery is receiving external power.

The main battery is charged/recharged when the MX9 is docked in a powered cradle or directly cabled to an external power source.



The backup battery draws power from the Main battery to maintain a charge. The backup battery voltage and percentage of power fluctuate continuously.

When there is no Main battery in the unit, the backup battery begins to discharge as it maintains RAM and other vital settings. After a Main battery is installed, the backup battery begins to draw power from the Main battery again.

Note: Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.

Certificates

Start > Settings > Control Panel > Certificates

Manage digital certificates used for secure communication.

Note: Digital certificates are date sensitive. If the date on the MX9 is incorrect, wireless authentication will fail.



The Certificates stores lists the certificates trusted by the MX9 mobile device user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

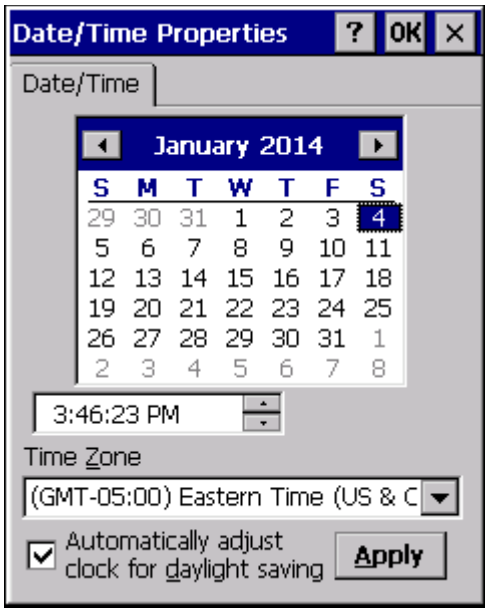
Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

Date / Time

Start > Settings > Control Panel > Date/Time - or - Time in Desktop Taskbar

Use this MX9 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Setting	Default
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled


Date/Time Properties
?
OK
Date/Time
January 2014
S M T W T F S
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
3:46:23 PM
Time Zone
(GMT-05:00) Eastern Time (US & C
Automatically adjust clock for daylight saving
Apply

There is very little functional change from general desktop or laptop Date/Time Properties options.

Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear.

The Sync button activates a utility that will set the clock using a network time server.

Device Management

Start > Settings > Control Panel > Device Management

Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.



Specify the server name or IP address of management server and tap the check box if a secure connection is to be used.

Refer to the Microsoft.com website for more information on device management for Windows CE equipped devices.

Dialing

Start > Settings > Control Panel > Dialing

Set dialup properties for internal modems. Honeywell does not support or supply internal modems in the MX9.

Setting	Default
Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)

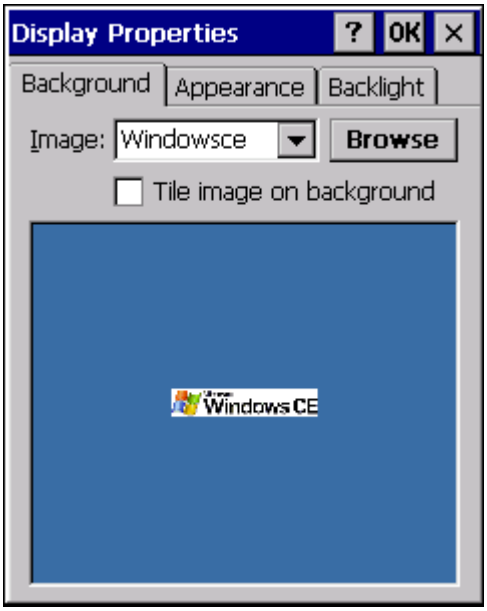
Display

Start > Settings > Control Panel > Display

The display might also called the touch screen. Select the desktop background image and appearance scheme for the MX9. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power. Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

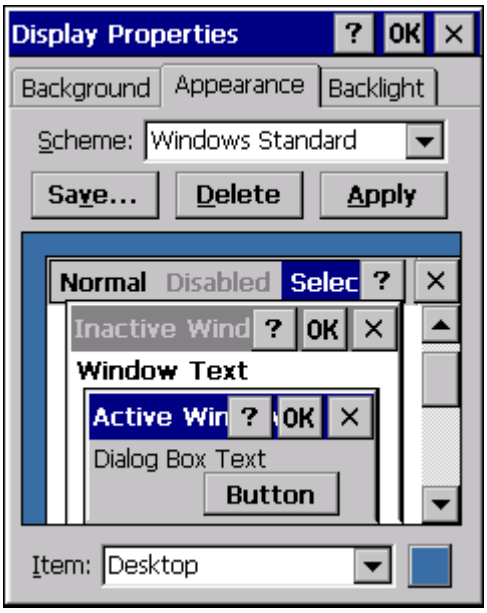
Setting	Default
Background	
Image	Windows CE
Image on background	Disabled
Appearance	
Schemes	Windows Standard
Backlight	
Battery power and user idle	3 seconds
Battery power and System idle	15 seconds
Battery power, idle, Suspend	5 minutes
External power and user idle	2 minutes
External power and System idle	2 minutes
External power, idle, Suspend	2 minutes
Backlight Brightness	Maximum

Background



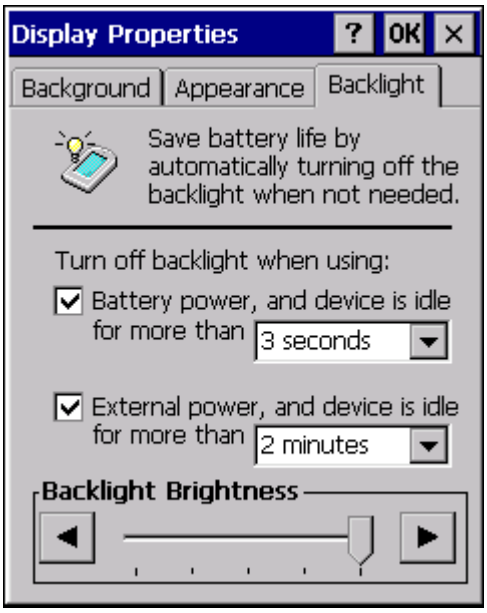
There is very little change from general desktop PC Display Properties / Background options. Select an image from the drop down list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance



There is very little change from general desktop PC Appearance options. Select a scheme from the drop down list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight



The backlight settings use the default timeouts and is synchronized to the User Idle setting in the Schemes tab in the Power control panel. When the backlight timer expires, the touch screen backlight is dimmed, not turned off. When both checkboxes are unchecked, the backlight never turns off (or dims). Default values are 3 seconds for Battery, 2 minutes for External and both the check boxes are enabled.

When the keypad backlight is set to Follow the touch screen backlight, the keypad backlight turns off when the touch screen backlight dims.

Adjust backlight brightness by moving the slider. Changes are in effect immediately.

Touch screen display backlight brightness adjust mode is entered by pressing the Blue + Scan key combination.

After this, the up and down arrow keys brighten or dim the backlight. Pressing any key other than up arrow or down arrow exits the brightness adjustment mode.

Additional characteristics:

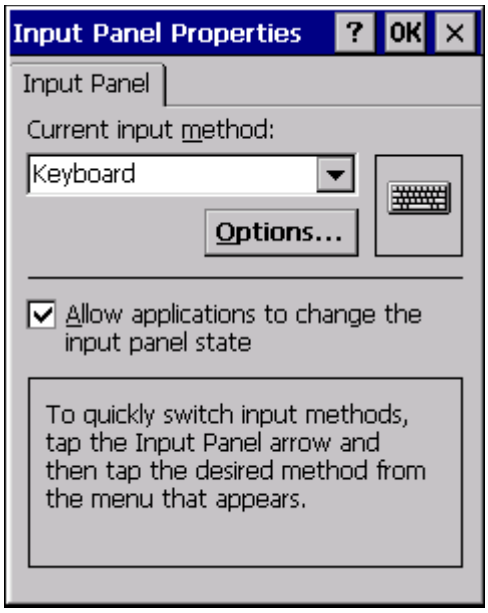
- There is no separate brightness level indication except for the actual brightness of the display.
- Once the maximum (or minimum) brightness is reached by repeated presses of the up (or down) key, the display will cease getting brighter (or dimmer) and saturate at that maximum (or minimum brightness).
- Continuously pressing the up or down arrow keys does not cause an automatic repeat of the up (or down) arrow key.
- The brightness setting is stored in the registry and is recalled at power on.
- The number of steps from maximum brightness to minimum dimness is five. At minimum dimness level, the display is still viewable.

Input Panel

Start > Settings > Control Panel > Input Panel

Set the current MX9 keys and data input method.

Setting	Default
Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options button	
Keys	Small keys
Use gestures	Disabled


Input Panel Properties
?
OK
Input Panel
Current input method:
Keyboard
Options...
Allow applications to change the input panel state
To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.

Use this panel to make the Input Panel (on-screen keyboard) or the physical keypad primarily available when entering data on any screen. Selecting Keyboard enables both. Tap the Options button to set the size of the keys displayed on-screen and whether Transcriber gestures are enabled or disabled.

Internet Options

Start > Settings > Control Panel > Internet Options

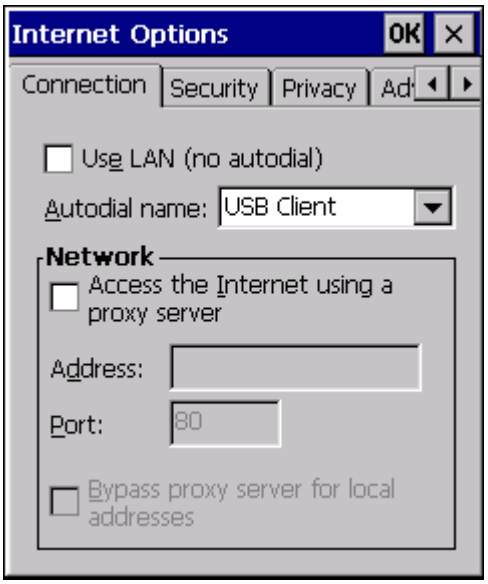
Set options for MX9 Internet connectivity. Select a tab. Tap the ? button for help using Windows CE Help installed in your mobile device. Adjust the settings and tap the OK button. The changes take effect immediately.

Setting	Default
General tab	
Start Page	http://www.honeywellaidc.com/
Search Page	http://www.google.com
User Agent	Default (Windows CE)
Cache Size	512Kb
Clear Cache	Button enabled
Clear History	Button enabled
Connection tab	
Use LAN	Disabled
Autodial Name	USB Client
Proxy Server	Disabled
Bypass Proxy	Disabled
Security tab	
Internet	Default site
Privacy tab	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced tab	
Stylesheets	Enabled
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups tab	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Security Tab

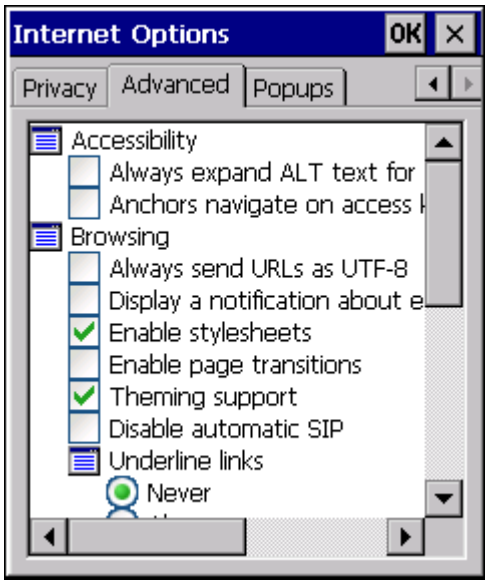
Use the Settings button to set ActiveX control, scripting and plug-in behavior for each zone (Internet, Local intranet, Trusted Sites, Restricted Sites). Use the Site button to add sites to each zone.

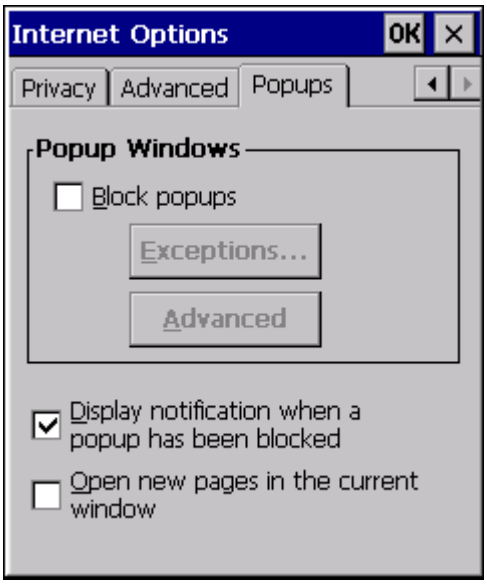

Internet Options
OK
General
Connection
Security
Start Page:
http://www.honeywell.com
Search Page:
http://www.google.com
User Agent (requires browser restart):
Default (Windows CE)
Cache Size (in KB):
512
Clear Cache
Clear History


Internet Options
OK
Connection
Security
Privacy
Use LAN (no autodial)
Autodial name:
USB Client
Network
Access the Internet using a proxy server
Address:
Port:
80
Bypass proxy server for local addresses


Internet Options
OK
Security
Privacy
Advanced
Internet
Local intranet
Trusted site
Internet
This zone contains all Web sites you haven't placed in other zones
Sites...
Settings...


Internet Options
OK
Privacy
Advanced
Popups
Cookies
First-party
Third-party
Accept
Block
Prompt
Always allow session cookies


Internet Options
OK
Privacy
Advanced
Popups
Accessibility
Always expand ALT text for
Anchors navigate on access
Browsing
Always send URLs as UTF-8
Display a notification about e
Enable stylesheets
Enable page transitions
Theming support
Disable automatic SIP
Underline links
Never

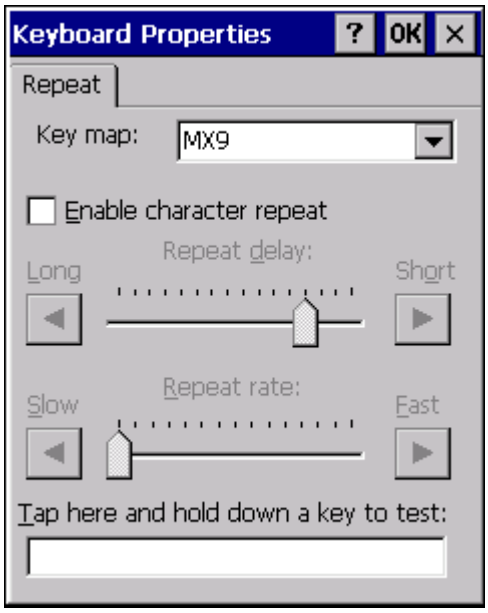

Internet Options
OK
Privacy
Advanced
Popups
Popup Windows
Block popups
Exceptions...
Advanced
Display notification when a popup has been blocked
Open new pages in the current window

Keyboard

Start > Settings > Control Panel > Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Setting	Default
Repeat Tab	
Key map	Default (or Default MX9)
Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



Select a key map using the drop down list. Adjust the character repeat settings and tap the OK button to save the changes.

When new key maps, or fonts, are added to the registry, they are available immediately and the font name is in the Keyboard Properties Key map drop down list. Only one font at a time can be selected. The fonts affect the screen display, they do not affect any virtual (touch screen) key taps.

See **About > Software > Language** tab for the name of any installed fonts.

Languages and Fonts

Fonts are available in the following languages (in separate part numbers) for each language: Simplified Chinese, Traditional Chinese, Korean, Japanese.

Tahoma font is on every unit and includes English (default), European (French, Spanish, German, Portuguese), Scandinavian languages, Arabic, Cyrillic, Greek, Hebrew, and Thai.

See Regional Settings for instruction for setting User Interface Language and Default Input Language.

KeyMap

Start > Settings > Control Panel > KeyMap

Use this control panel option to assign key functions to mappable keys available on your MX9, determine application launch sequences and program command Run sequences.

Note: KeyMap Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

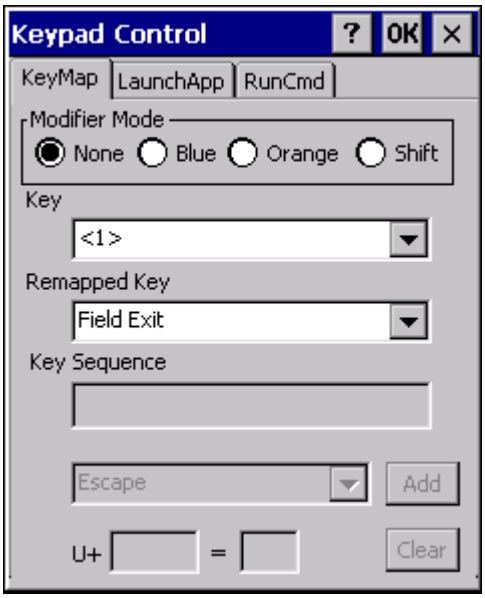
Setting	**Default**	
KeyMap		
Modifier Mode	None	
Edit String	Field Exit	String – Empty
Launch		
App1	Empty	
App2	Empty	
App3	Empty	
App4	Empty	
App/Opt	EXE	
RunCmd		
Cmd1	Empty	
Cmd2	Empty	
Cmd3	Empty	
Cmd4	Empty	
File/Parm	FILE	

The KeyPad panels can be used to perform the following functions:

- Remap a Single Key (page 5-32).
- Remap a Key to a Unicode Value (page 5-32).
- Remap a Key Sequence (page 5-32) to remap a key to a string of up to 16 keys or Unicode values in any combination.
- Remap a Key to a Sequence of Unicode Values (page 5-33).
- Remap an Application (page 5-33) to remap a key to launch a user-selected application.
- Remap a Command (page 5-33).

Note: KeyPad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

KeyMap Tab



Assign settings by tapping radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

Remap a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select the value from the remapped key from the Remapped Key pulldown list.
4. Tap **OK** to save the result and close the Keypad Control.

Remap a Key to a Unicode Value

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Unicode from the Remapped Key pulldown list.
4. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
5. Tap **OK** to save the result and close the control panel.

Remap a Key Sequence

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Key Sequence from the Remapped Key pulldown list.
4. Select the first key for the multiple key sequence from the pulldown list.
5. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box. Repeat this step until all keys desired have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
6. Tap **OK** to save the result and close the Keypad Control.

Note: A key can only be used once in a multiple key sequence. For example, an F1 key added to a key sequence means an F1 key cannot be used again in the same key sequence.

Remap a Key to a Sequence of Unicode Values

Up to 16 Unicode values may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Key Sequence from the Remapped Key pulldown list.
4. Select Unicode from the Key Sequence pulldown list.
5. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
6. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box.
7. Repeat steps 4 through 6 until all desired characters have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
8. Tap **OK** to save the result and close the control panel.

Remap an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Launch App1-4 from the remapped key from the Remapped Key pulldown list.
4. Tap on the LaunchApp tab.
5. Make sure the EXE radio button is selected.
6. In the text box (App1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.
7. If any parameters are needed for the application, tap on the OPT radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.
8. Tap **OK** to save the result and close the Keypad Control.
9. If the KeyMap tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

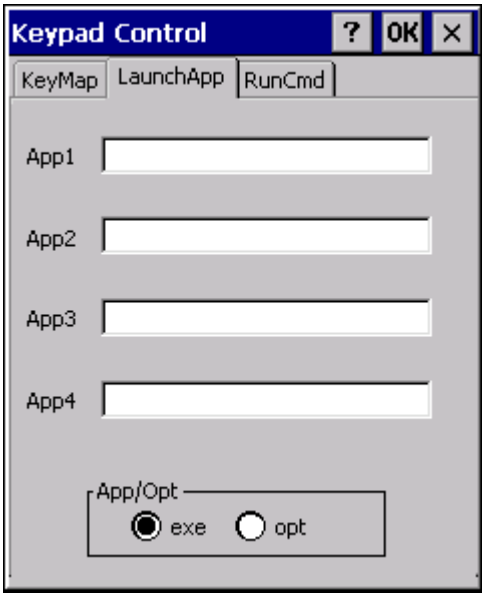
Remap a Command

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select RunCmd 1-4 from the remapped key from the Remapped Key pulldown list.
4. Tap on the RunCmd tab.
5. Make sure the FILE radio button is selected.
6. In the text box (Cmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.
7. If any parameters are needed for the command, tap on the PARM radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.
8. Tap **OK** to save the result and close the Keypad Control.
9. If the KeyMap tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the MX9 emits a single beep, if the launch is successful, it is silent.



The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g., App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

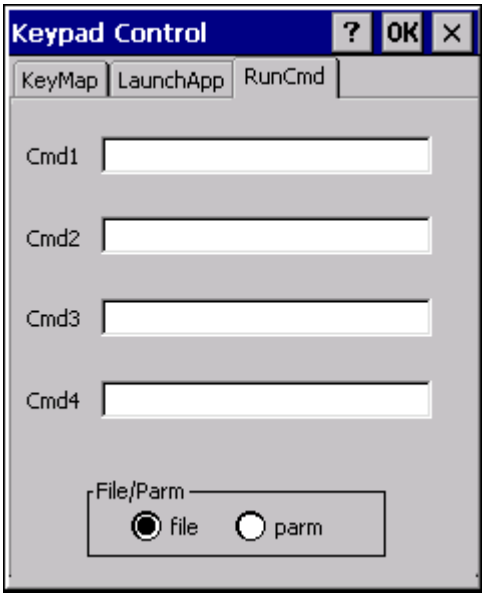
Tap the OK button when finished. The changes take effect immediately.

The result of the application (exe) and options (opt) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd Tab

The default for all text boxes is Empty, Null or “ ”. The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the MX9 emits a single beep, if the launch is successful, the mobile device is silent.



The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g., Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.

Tap the OK button when finished. The changes take effect immediately.

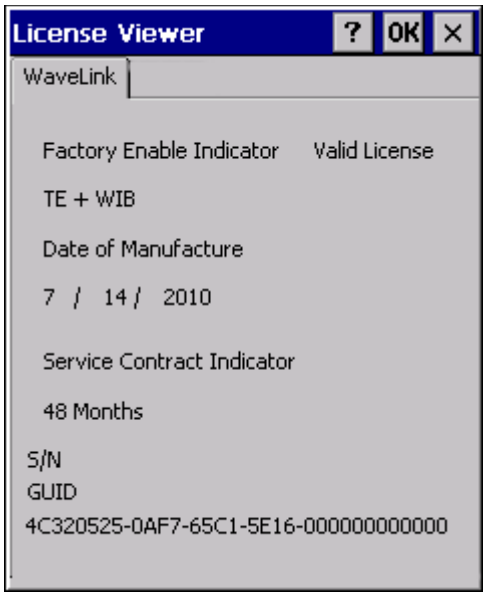
License Viewer

Start > Settings > Control Panel > License Viewer

Use this option to view software license registration details, and service contract length for a MX9. Information on the License Viewer tabs is unique for each MX9.

Note: Following image is a sample screen.

Your License Viewer control panel may show more tabs, e.g., RFTerm, depending on the number of software applications running on the MX9 that require a license.



Software and driver version information is located in the About control panel. Copyright information is located in the System control panel.

Mixer

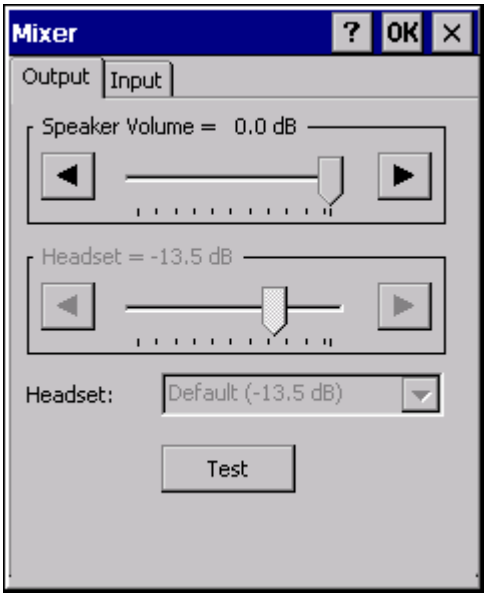
Start > Settings > Control Panel > Mixer

The MX9 has a speaker and a microphone. They are active when a headset is not connected to the device. The microphone is located to the left of the oval logo at the top of the unit. The speaker (audio) is located above the keypad.

Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output. Headsets can be enabled, disabled and selected using these panels.

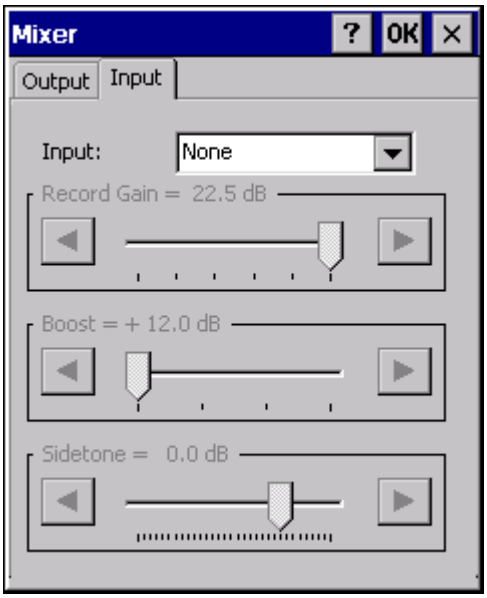
Setting	Default
Output	
Speaker Volume	0 dB
Headset Volume	-13.5dB
Headset Selection	Default
Input	
Input Selection	None
Record Gain	0 dB
Record Boost	+12 dB
Sidetone	0 dB

Output Panel



Tap and hold the Output sliders and move them either left or right, or tap the left and right arrows, to adjust Speaker volume decibel level. Tap the drop down list arrow to select the type of headset currently attached to the unit. This will load a predetermined limit value; the headphone setting cannot exceed the predetermined values.

Input Panel



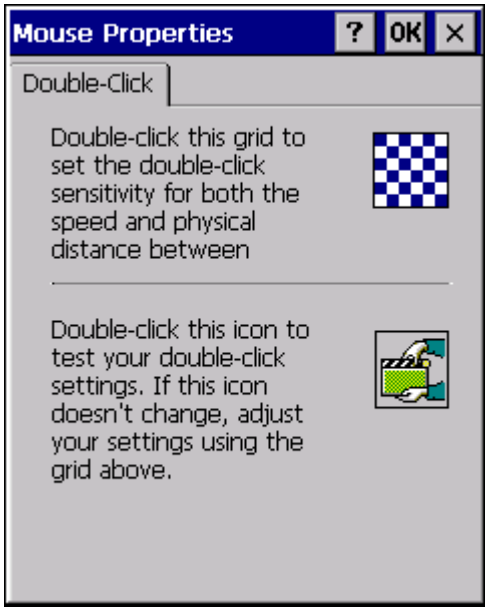
To enable the headset, select Headset in the Input Selection combo box. To disable the headset, select None in the Input Selection combo box.

Note: The list of input selections and headset selections is stored in the registry. Both WAN and Bluetooth are included in the input list in the registry, but with the disabled flag set, they do not appear in the list.

Mouse

Start > Settings > Control Panel > Mouse

Use this option to set the double-tap sensitivity for stylus taps on the MX9 touch screen.


Mouse Properties
?
OK
Double-Click
Double-click this grid to set the double-click sensitivity for both the speed and physical distance between
Double-click this icon to test your double-click settings. If this icon doesn't change, adjust your settings using the grid above.

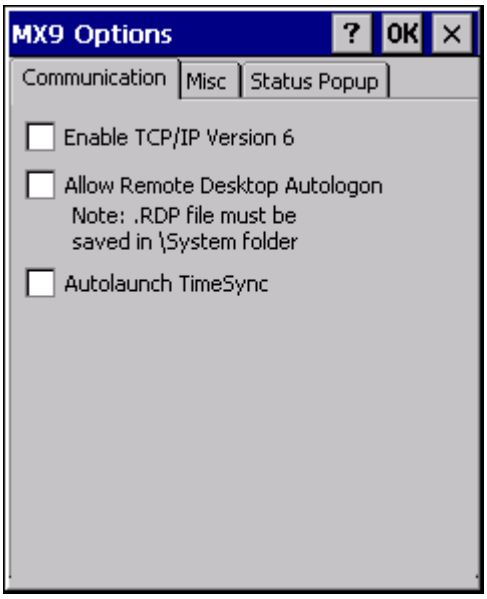
MX9 Options

Start > Settings > Control Panel > MX9 Options

Set options unique to your device, such as keypad backlight, Status Popup taskbar icon display and CapsLock. It may be necessary to warmboot the MX9 after making desired changes. A pop up window imforms if a warmboot is required.

Communication Tab

Options on this tab configure communication options for the MX9.



Enable TCP/IP Version 6

By default, IPv6 is disabled on the MX9. Tap this check box to enable IPv6.

Allow Remote Desktop Autologon

By default, Remote Desktop Autologon is disabled. Tap this check box to enable Remote Desktop Autologon.

Note: The .RDP file must be saved in the \System folder. When prompted, use the Save As button to save the .RDP file is the \System directory. If the .RDP file is saved in the default root folder location, the .RDP file will not persist across a warmboot.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the MX9. To enable TimeSync to run automatically on the MX9, tap this check box.

Synchronize with a Local Time Server

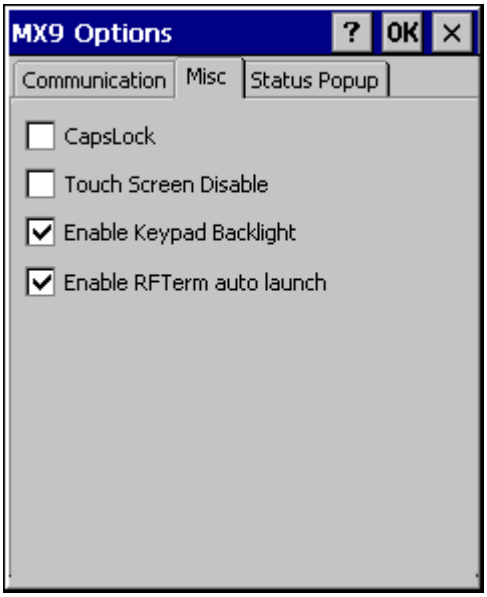
By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the **My Device > Windows** folder on the mobile device to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the **My Device > System** folder on the mobile device.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Misc Tab

Options on this tab configure device specific options. Note that options not available on the MX9 are dimmed or grayed out.



CapsLock

By default, CapsLock is disabled after a warmboot. To enable CapsLock after a warmboot, tap this check box.

Touch Screen Disable

By default, the MX9 touch screen is enabled. To disable the touch screen after a warmboot, tap this check box.

Enable Keypad Backlight

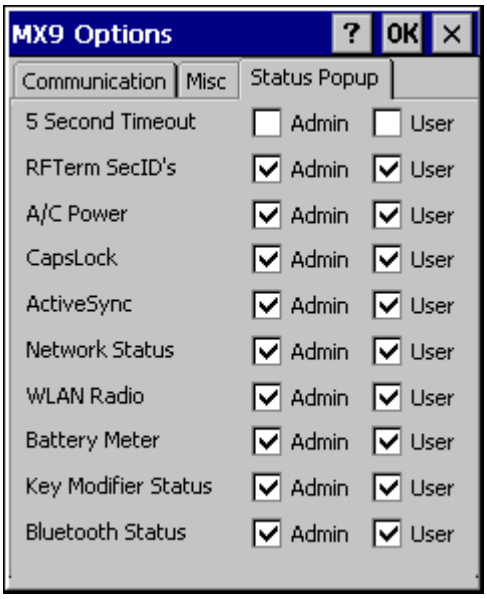
The keypad backlight default setting is to follow the display backlight setting until it is changed by the user. Uncheck the check box to disable the keypad backlight.

Enable RFTerm Auto Launch

This option is enabled by default. This option, when disabled (unchecked) stops RFTerm from launching at bootup. When RFTerm is not installed or has not been added to the registry Launch sequence, this check box is ignored at bootup.

Status Popup Tab

Options on this tab configure the Status Popup window. When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it. It is closed by pressing the assigned Status User or Status Admin key sequence.



Using the Key mapping control panel, the System Administrator must first assign a Status User key sequence for the end-user when they want to toggle the Status Popup Window on or off.

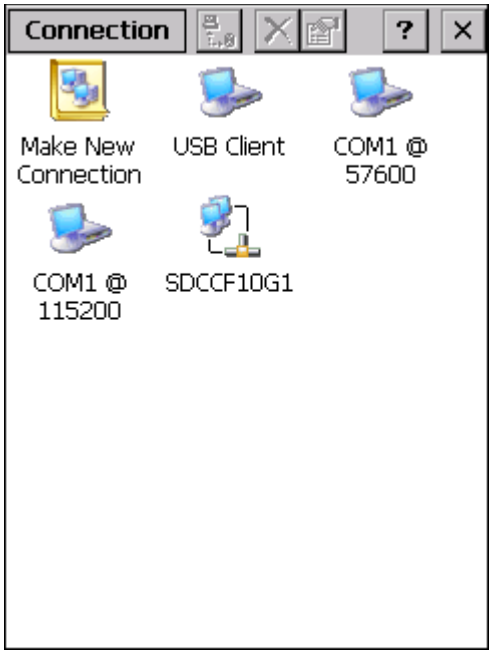
The System Administrator must also assign a Status Admin key sequence to perform the same function. Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g., AC Power, ActiveSync, WLAN radio, CapsLock, Network status, Bluetooth status, etc.

The default for the User and Admin status popup windows is to show all status information. The 5 second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

Network and Dialup Options

Start > Settings > Control Panel > Network and Dialup Connections

Set MX9 network driver properties and network access properties. Select a connection to use, or create a new connection.



Creating a New Connection

1. On the mobile device, select **Start > Settings > Control Panel > Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the Direct Connection radio button. Tap the **Next** button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the Port Settings tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap **OK**.
8. TCP/IP Settings should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the Remote Networking window.
10. To activate the new connection select **Start > Settings > Control Panel > PC Connection** and tap the **Change Connection…** button.
11. Select the new connection. Tap **OK** twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Tap the desktop **Connect** icon to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Network Capture

Start > Settings > Control Panel > Network Capture

Note: Verify the date and time before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities. Two types of logging are configurable:

Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

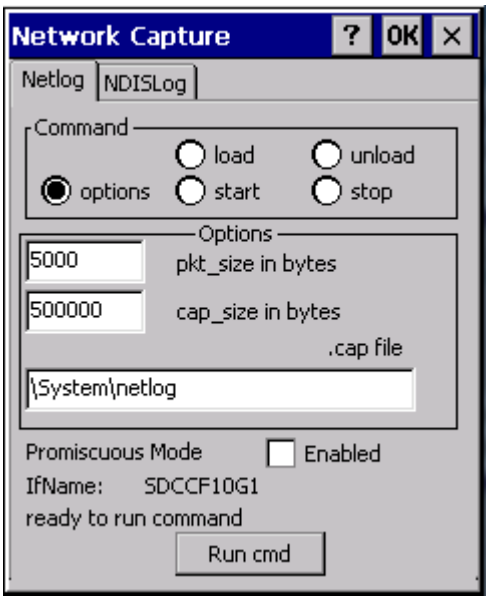
NDISLog monitors the the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

Setting	Default
Netlog	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuous Mode	Disabled
NDISLog	
Command	stop
file	\ndislog.txt

Netlog Tab

Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warmboot.
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user interaction is required.



Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called **load** and **stop**. Default is 5000.
cap_size in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called **load** and **stop**. Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called **load** and **stop**. Default is \netlog.

Run cmd

Performs the command selected.

NDISlog Tab

NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.



Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

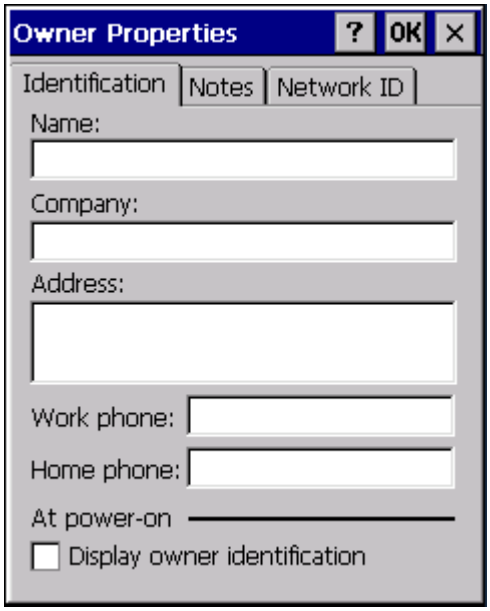
Performs the selected start or stop command.

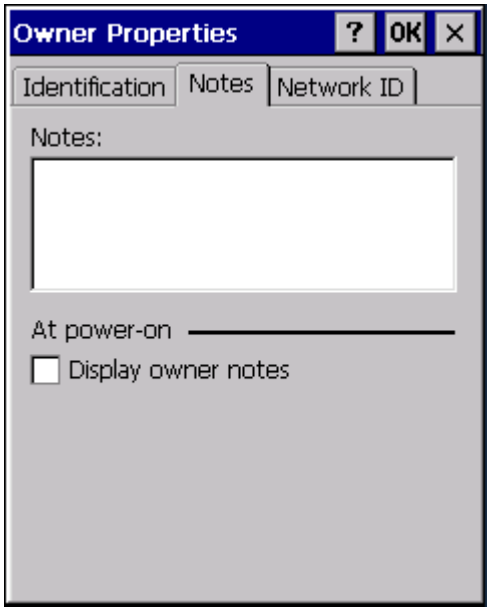
Owner

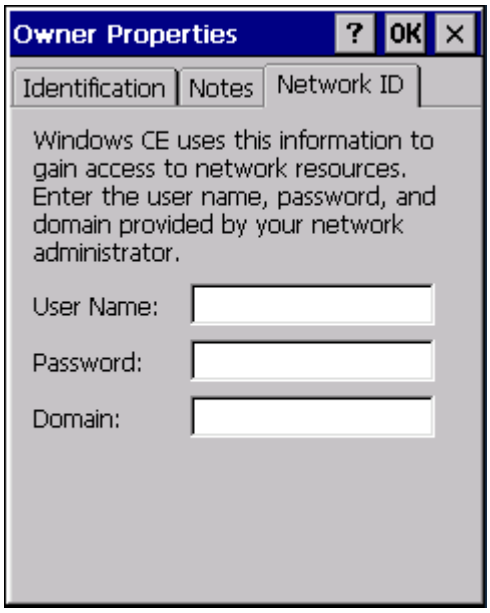
Start > Settings > Control Panel > Owner

Set the MX9 owner details. The Network ID is used when logging into a remote network.

Setting	Default
Identification	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes	
Notes	Blank
Display notes at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank







Enter user name, password and domain to be used when logging into network resources.

Password

Start > Settings > Control Panel > Password

Use this panel to set MX9 user access to control panels and power up password properties.

Important: This password must be entered before performing a Load Factory Defaults on the Registry control panel.

Contact Technical Assistance (page 15-1) if entering a power-on or screen saver password does not allow you to disable this password protection or perform a Load Factory Defaults.

Setting	Default
Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled



Enter the password in the Password text box, then press Tab and type the password again to confirm it.

Enable the power-on check box and, if desired, the screensaver check box. A changed/saved password is in effect immediately.

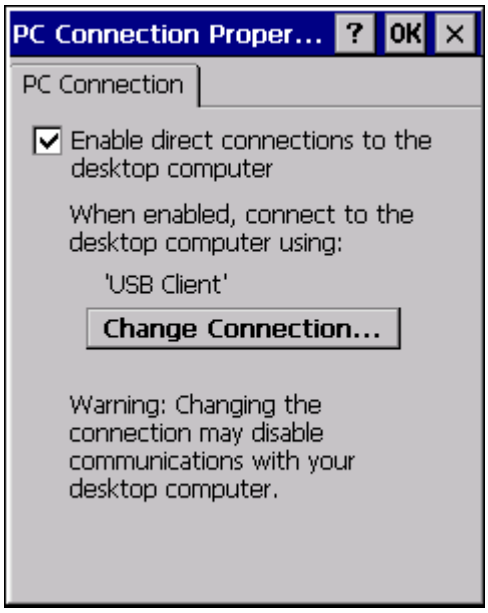
- The password and password settings are saved during a warm boot and a cold boot.
- The screensaver password affects the Remote Desktop screensaver only.
- After a password is assigned and saved, each time a **Settings > Control Panel** option is selected, the user will be required to enter the password before the Control Panel will open.
- The screensaver password is the same as the power-on password. They are not set independently.
- A screensaver password cannot be created without first enabling the “Enable password protection at power-on” check box.
- The screensaver password is not automatically enabled when the “power-on” check box is enabled.

PC Connection

Start > Settings > Control Panel > PC Connection

Use these options to control a cabled connection (USB, serial) between the MX9 and a nearby desktop/laptop computer.

Setting	Default
Enable direct connection	Enabled
Connect using	USB Client


PC Connection Proper...
?
OK
PC Connection
Enable direct connections to the desktop computer
When enabled, connect to the desktop computer using:
'USB Client'
Change Connection...
Warning: Changing the connection may disable communications with your desktop computer.

Unchecking the Enable direct connections check box disables ActiveSync on the MX9.

Tap the Change Connection button to change the direct connect setting.

Tap the drop down box to view a list of pre-configured connection settings.

Peripherals

Start > Settings > Control Panel > Peripherals

These panels are used to enable and disable the touch screen and scanner window heaters, and they are also used to set the time limit for the flashlight. Using the GPS tab, power to the GPS can be toggled on or off.

Setting	Default
Heaters	
Touch screen heater	Enabled
Scanner window heater	Enabled
Flashlight	
Turn flashlight off after	1 minute
GPS	
GPS Power	ON when installed / OFF when not installed

Heaters Tab

Note: Setting has no effect if the heater is not installed.



Tap the radio button to enable or disable the touch screen and/or scanner aperture (window) heater.

Flashlight Tab

Note: Setting has no effect if the flashlight is not installed.



Select an option to set the timeout for the flashlight. Options are:

- 1 minute
- 2 minutes
- 3 minutes

GPS Tab



GPS presence is displayed on the GPS panel. Power can be toggled on or off only when a GPS is installed. The default setting is Off.

Power

Start > Settings > Control Panel > Power

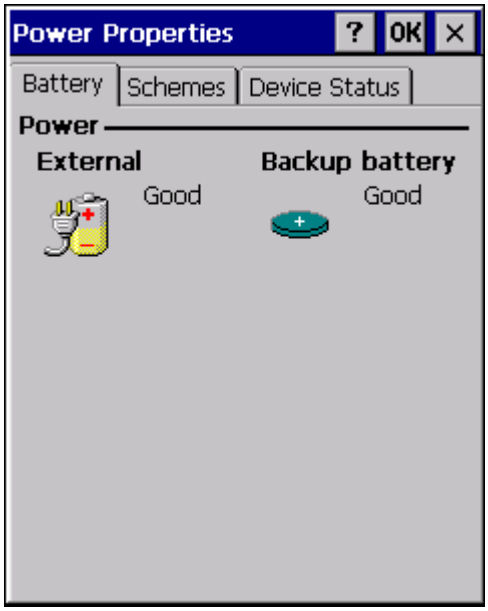
The MX9 power mode timers are cumulative.

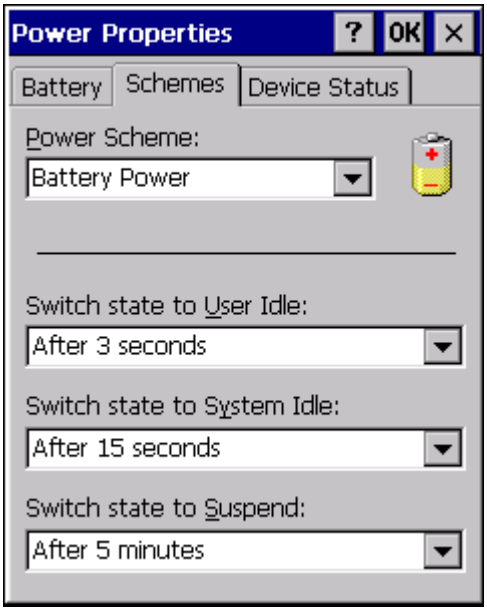
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the count-down after the System Idle timer has expired.

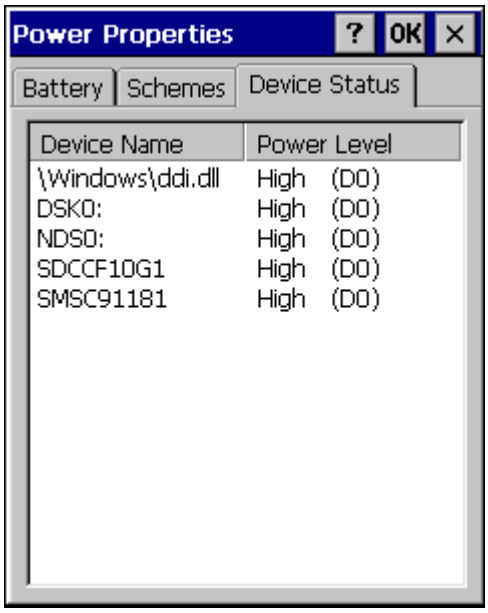
When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The **Display > Backlight** setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Setting	Default
Schemes Tab	
Battery Power - User Idle Timeout	3 seconds
Battery Power - System Idle Timeout	15 seconds
Battery Power - Suspend Timeout	5 minutes
AC Power - User Idle Timeout	2 minutes
AC Power - System Idle Timeout	2 minutes
AC Power - Suspend Timeout	5 minutes







Because of the cumulative effect, and using the Battery Power Scheme Defaults listed:

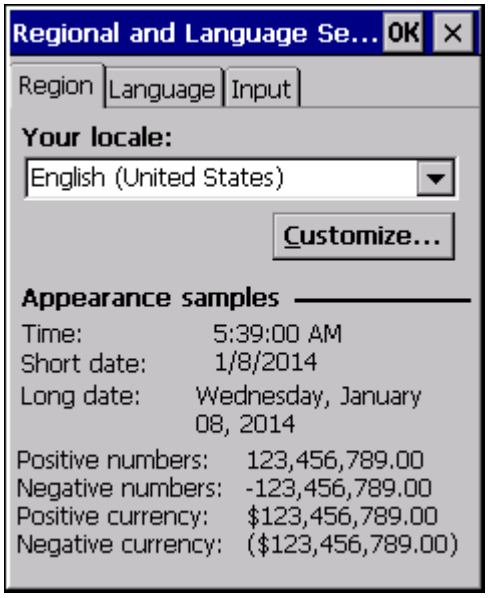
- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.
- If the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

Regional and Language Settings

Start > Settings > Control Panel > Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the MX9 user interface language and the default input language.

Setting	Default
Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US



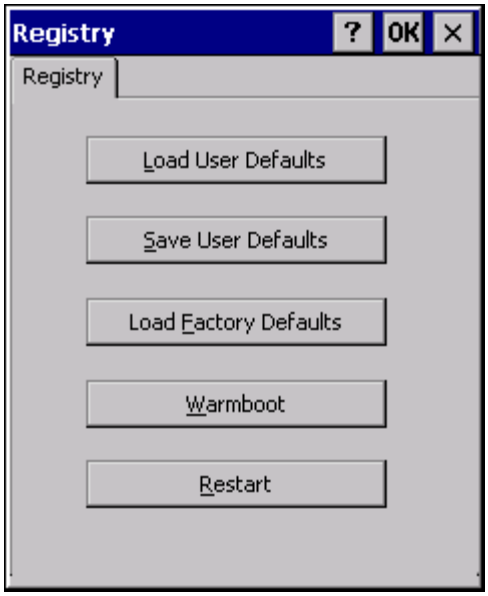



Regional and Language Se...
OK
Region
Language
Input
Default Input Language:
Select the input language to use when you start your device.
English (United States)-US
Installed Input Languages:
Select input languages you plan to use.
English (United States)-US

Registry

Start > Settings > Control Panel > Registry

Choose an MX9 software reload scheme.



Load User Defaults Button

When tapped, a standard load file dialog is opened, to allow the user to pick a Registry Save (.RSG) file. The applet then copies the specified User registry file to the Active registry. The user is asked to verify a reboot, and then the applet does a warmboot to activate the new registry.

Load User Defaults takes 20 seconds from SD card, or 10 seconds from internal flash.

Save User Defaults Button

When tapped, a standard Save File dialog is opened, to allow the user to name the Registry Save (.RSG) file. The applet then copies the Active registry to the specified User registry file.

Save User Defaults takes 30 seconds to save to SD card, or 10 seconds to save to internal flash.

Load Factory Defaults Button

The applet copies the Factory Default registry from the OS to the Active registry (by deleting the current registry). The user is asked to verify a reboot, and then the applet does a restart to activate the factory default registry. If a user password has been set, the applet warns the user that the password will be erased, and asks them to enter it before the reboot is allowed.

Warmboot Button

When tapped, the OS does a registry flush (Active registry saved to Flash registry hive), and then a warmboot.

Restart Button

When tapped, the OS does a registry flush, and then a restart.

Remove Programs

Start > Settings > Control Panel > Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

Select a program and tap Remove. Follow the prompts on the screen to uninstall MX9 user-installed only programs. The change takes effect immediately.

Files in the My Documents folder are not removed using this option.

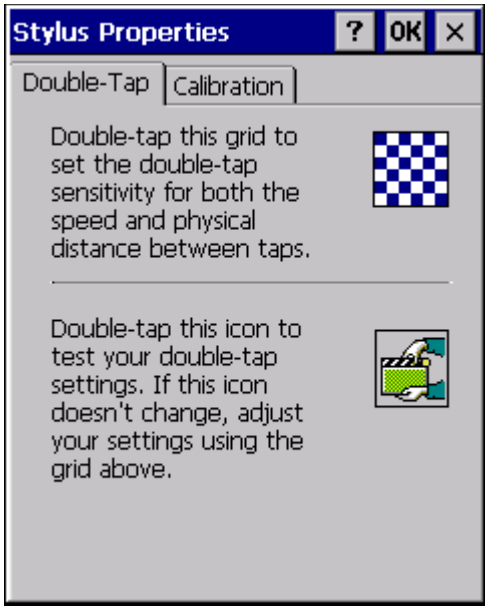


Note: Do not remove Honeywell-installed programs using this option. Contact Technical Assistance for help if Honeywell installed programs must be deleted.

Stylus

Start > Settings > Control Panel > Stylus

Use this control panel option to set stylus double-tap sensitivity properties and calibrate the MX9 touch panel when needed.


Stylus Properties
?
OK
Double-Tap
Calibration
Double-tap this grid to set the double-tap sensitivity for both the speed and physical distance between taps.
Double-tap this icon to test your double-tap settings. If this icon doesn't change, adjust your settings using the grid above.



Double Tap Tab

Follow the instructions on the screen and tap the OK button to save any double tap changes.

Calibration Tab

Calibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To begin, tap the Recalibrate button on the screen with the stylus. Press and hold the stylus on the center of the target as it moves around the screen. Press the Enter key to keep the new calibration setting or press the Esc key to revert to the previous calibration settings.

System

Start > Settings > Control Panel > System

Use these MX9 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Setting	Default
General	No user interaction
Memory	1/3 storage, 2/3 program memory
Device Name	Unique to equipment type
Device Description	Unique to equipment type
Copyrights	No user interaction

General Tab



System

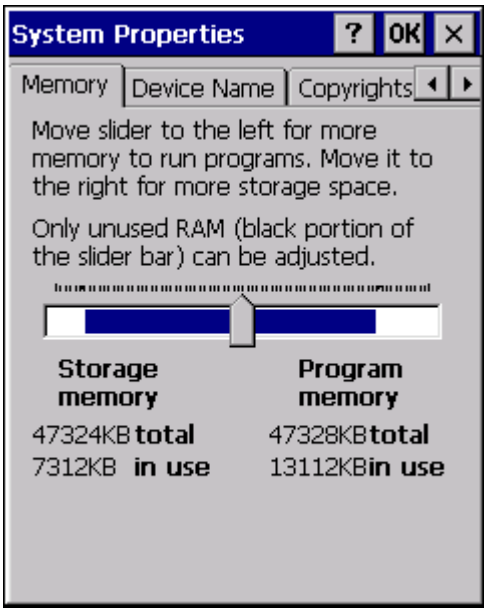
This screen is presented for information only. The System parameters cannot be changed by the user.

Computer

The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab



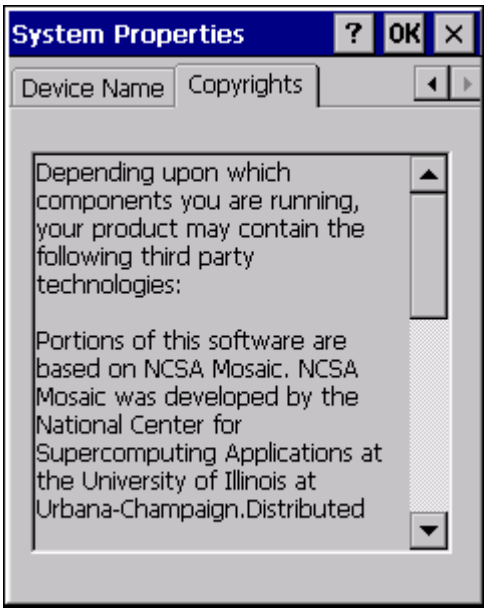
Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap **OK** to save the changes. This information is used to identify the MX9 to other computers and devices.

Copyrights Tab


System Properties
?
OK
Device Name
Copyrights
Depending upon which components you are running, your product may contain the following third party technologies:
Portions of this software are based on NCSA Mosaic. NCSA Mosaic was developed by the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.Distributed

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Terminal Server Client Licenses

Start > Settings > Control Panel > Terminal Server Client Licenses



Any licenses stored on the MX9 appear in the drop down list. Select a license and tap the Close button. The license is available for use immediately.

Volume and Sounds

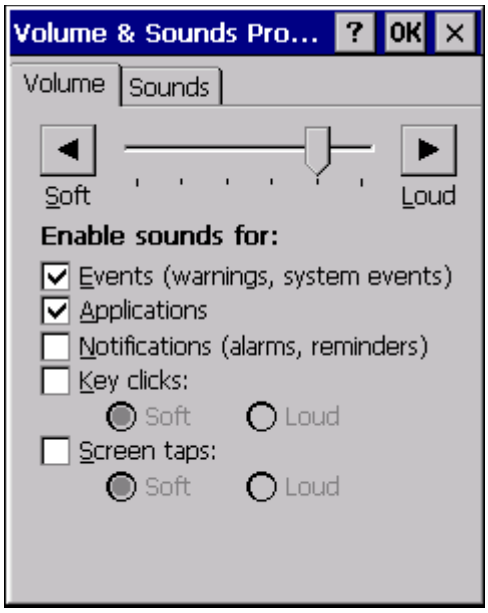
Start > Settings > Control Panel > Volume & Sounds

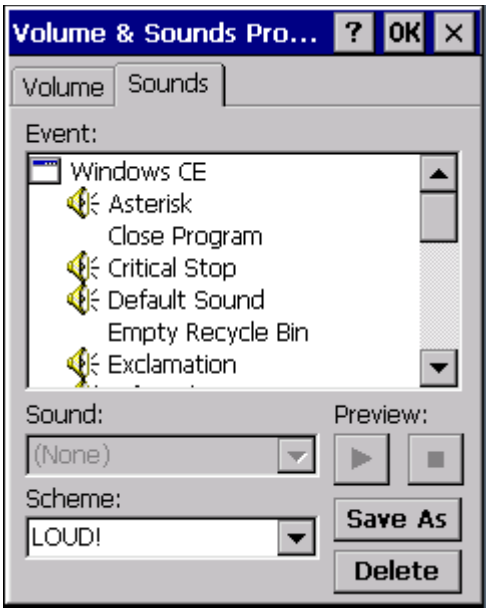
Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options. You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft. As the volume scrollbar is moved between Loud and Soft, the MX9 emits a tone each time the volume increases or decreases.

Volume must be enabled when you want to adjust volume settings using keypad keys.

Setting	Default
Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!





The volume setting is stored in the registry and is recalled at power on.

Note: Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned bar code data by the bar code processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the MX9 is a single beep, and a bad scan sound is a double beep.

Wi-Fi

Start > Settings > Control Panel > Wi-Fi

or

Tap the Summit Client Utility icon

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your MX9. See Wireless Network Configuration (page 10-1) for more information.

WWAN

Start > Settings > Control Panel > WWAN

These panels can be used to set the parameters for the Wireless Wide Area Network (WWAN) on the MX9. The WWAN is a form of wireless network that utilizes a cellular network instead of the spread spectrum network most used by Wireless Local Area Networks (WLAN).

Setting	**Default**
Connection tab	
Status	Not Connected
Connect button	Dimmed
Admin Login button	Enabled
Network tab	
Phone, Username, Password, APN	Blank
TCP/IP tab	
DHCP	Enabled, dimmed
DNS	Enabled, dimmed
Addresses	Pre-populated, dimmed
Security tab	
use Extensible Auth Protocol	Enabled
Autoconnect tab	
Automatically connect - turned On	Disabled, dimmed
Automatically reconnect	Enabled, dimmed
Admin tab	
Admin Factory Default Password	LXEWWAN
Enable Radio button	Dimmed
PIN (Personal Identification Number)	Enabled, Blank
PUK (Personal Unblocking Key)	Disabled, Dimmed

Initial Setup



1. Enable the radio by tapping the Admin Login button on the Connection panel (the Connect button is dimmed).
2. Enter the password in the Admin Password Entry popup text box. The default case-sensitive password is LXEWWAN. The Connect button is enabled.
3. Tap the Connect button to begin a connection with a WWAN.
4. Fill in the appropriate fields displayed on the remaining tab panels of the WWAN control panel.

Connection Tab

The Connect button controls Connect/Disconnect operation and the caption of the button changes based on the connection status. The Connect button is dimmed when the radio is disabled or absent.



Tap the Connect button to begin a connection with a WWAN. The button caption changes to Disconnect.

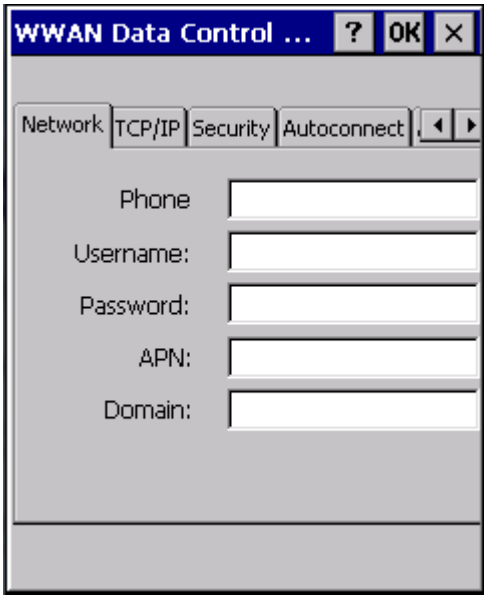
Tapping the Admin Login button displays the Admin Password Entry popup text box. After password entry is successful, the button caption changes to Admin Logout.

Entering an incorrect password causes an error message to be displayed.Enter the password in the popup text box and tap the OK button.



Admin Login causes all dimmed buttons and configurable fields on Network, TCP/IP, Autoconnect, and Admin tabs to be enabled.

Network Tab



Enter the following information for the MX9:

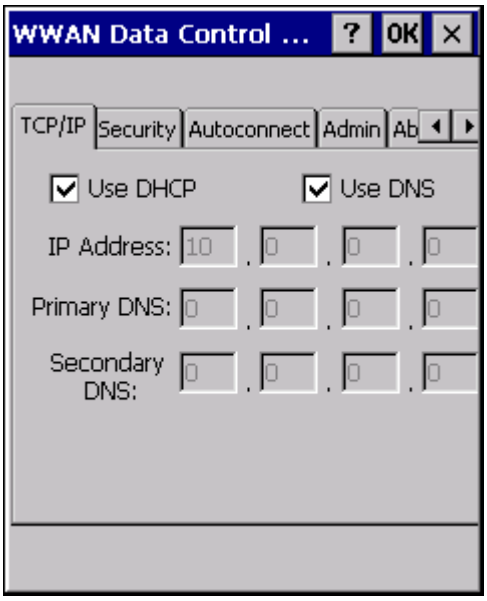
- Phone (data access number)
- Username
- Password
- APN (Access Point Name)

Note: Some fields may not require an entry. Contact your system administrator for the information needed.

TCP/IP Tab

The TCPIP tab contains a check box for indicating that TCP/IP parameters are to be obtained from the network DHCP server.

This tab also contains fields for entering a static IP address and the addresses of the primary and secondary DNS servers, if DHCP and DNS are not used.



Tap the check box to enable or disable DHCP and/or DNS. When the Use DHCP check box is enabled, the static IP address is disabled. When the Use DNS check box is enabled, the DNS address fields are disabled.

If DHCP and DNS are not used, enter the addresses for:

- Static IP Address
- Primary DNS server
- Secondary DNS server

Security Tab

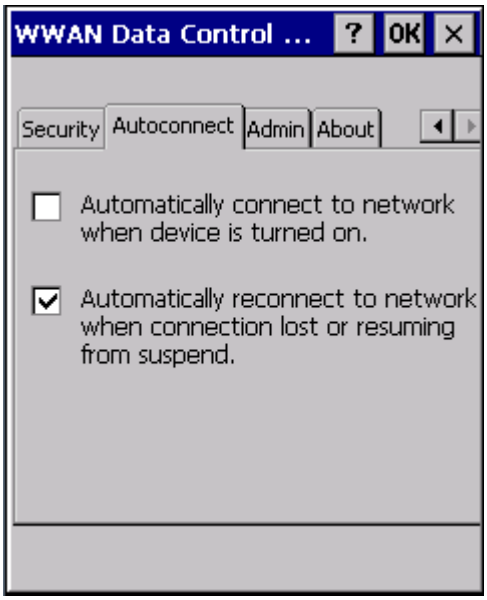
The Heading tab allows for entering and storing of security parameters for the WWAN connection. If security parameter are set using the Network and Dial-up Connections control panel, they are not stored and are reset when the MX9 is rebooted. Use this tab to ensure the settings are stored in the registry and persist across a warmboot or restart.



By default, EAP (Extensible Authentication Protocol) is enabled. If EAP is deselected, the other security options are then selectable.

Autoconnect Tab

The Autoconnect tab contains two checkboxes.



Automatically connect to network when device is turned on.

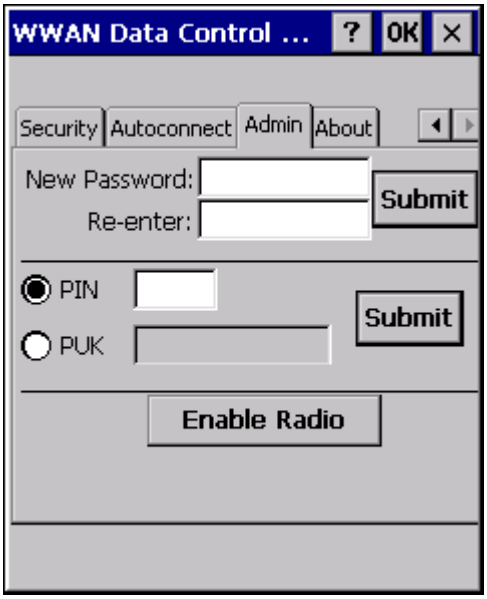
When this check box is enabled (checked) the radio automatically connects to the network when the device is turned on (power button is pressed).

Automatically reconnect to network when connection lost or resuming from suspend.

When this check box is enabled, the radio automatically attempts to reconnect to the network when it is resumed after being in the suspend state. Automatic reconnection applies whether Autoconnect is on or off.

Admin Tab

The Admin tab provides the ability to change the configuration password (see the Connection Tab (page 5-65)), enter Identification numbers for the SIM card, and provides a button to disable/enable the radio.



Password

Enter a new password, then re-enter the same password. Tap Submit to save the new password.

Tap the Enable Radio button to turn the radio On or Off. When the radio is Off, the Admin password will need to be entered before the radio can be set to On.

PIN (Personal Identification Number)

The PIN is a unique sequence of numbers stored on the SIM card.

If the radio is enabled and the SIM card requires a PIN, a connection will not occur until the PIN is entered successfully. After entering the PIN code, tap the Submit button. A message is displayed with either Success or the number of retries allowed before the SIM card PIN number entry is locked from further use.

If the radio is disabled, entering and submitting the PIN saves the PIN value on the MX9. The next time the radio is enabled and requires a PIN, the saved PIN will be sent and a PIN will not need to be entered again.

PUK (Personal Unblocking Key)

The PUK is a unique sequence of alpha characters displayed on the SIM card. A default PUK code is not available. After entering the PUK code, tap the Submit button. A message is displayed with either Success or the number of retries allowed before the SIM card PUK entry is locked from further use.

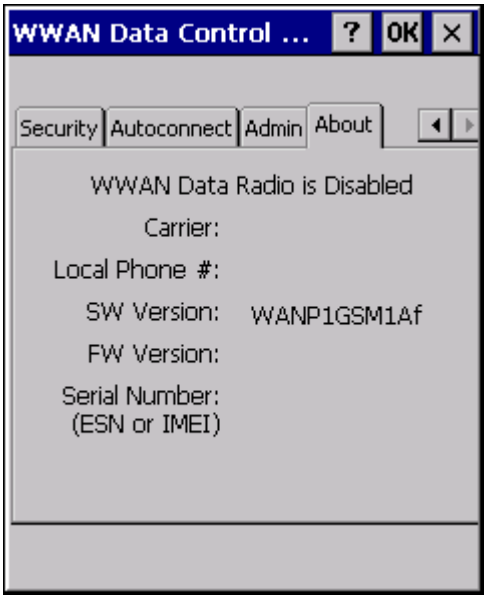
Enable/Disable Radio button

Tap the Enable Radio button to turn the radio On or Off. If the radio is currently enabled, the button is labeled Disable Radio. If the radio is currently disabled, the button is labeled Enable Radio.

About Tab

The About tab displays information about the WWAN radio and the current network connection. The About tab displays the SW Version, FW Version and Serial Number of the radio if there is a WAN radio installed in the device. the Local Phone Number shows the subscriber's own number from the SIM card. The current radio enable/disable status is displayed.

The Carrier entry displays the carrier configuration of the SIM card. In addition to the data shown in the dialog box below, the SW Version is displayed as well. The version matches the corresponding version in the **Start > Settings > Control Panel > About > Versions** dialog box. All fields in the About dialog box are read-only. This information is available to all users without requiring the configuration password.



Some of the information shown on this panel can be edited, after logging in, on previous panels:

- Enable Radio
- Carrier Name
- Local Phone Number

Using ActiveSync

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the MX9.

Requirement : ActiveSync (version 4.5 or higher for Windows XP) must be resident on the host computer. Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista or higher host computer. ActiveSync and Windows Mobile Device Center for the host computer is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync, you can synchronize information on your desktop computer with the MX9 and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Note: Contact Technical Assistance (page 15-1) for upgrade availability if your application or control panels are not the same as the application or control panels presented in this chapter.

MX9 without Touch Screen

The MX9 touch screen can be disabled. It may be easier to configure the MX9 using ActiveSync and HSM Connect (or LXEConnect) rather than using the MX9 keyboard only.

Initial Setup

The initial setup of ActiveSync must be made via a USB or serial connection. When there is a Connect icon on the desktop, this section can be bypassed.

Partnerships can only be created using direct serial or a USB cable connection.

After the partnerships are established, ActiveSync communication can be initiated using:

- USB
- Serial
- Wireless

Connect via USB

The default connection type is USB Client.

To change the connection type or to verify it is set to USB, select **Start > Settings > Control Panel > PC Connection**.

USB Client should be shown.

This will set up the mobile device to use the USB port. Tap **OK** and ensure the check box for “Allow connection with desktop computer when device is attached” is checked.

Tap **OK** to return to the Control Panel. If desired, any control panel windows may be closed.

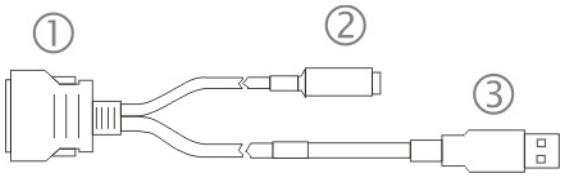
IMPORTANT – DO NOT PUT THE MX9 INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Connect the correct cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select “Connect” from the start menu.

Cable for USB ActiveSync Connection

MX9051CABLE - MX9 USB Client Cable Assembly (ActiveSync connection)

- Connect the I/O connector to the I/O port on the bottom of the MX9.
- The USB client type A plug on the MX9 cable connects to a USB port on a PC or laptop.
- It is not necessary to connect the power receptacle to the MX9 power adapter in order to use ActiveSync. Do not allow the device to enter Suspend while connected.



1. Connect to Input/Output port on MX9
2. Insert A/C adapter cable
3. Connect to host USB port

Serial Connection

The connection type must be changed to Serial 1 @ 57600.

To change the connection type select **Start > Settings > Control Panel > PC Connection**.

Tap the Change button. From the popup list, choose Serial 1 @ 57600.

This will set up the mobile device to use the serial port. Tap **OK** and ensure the check box for “Allow connection with desktop computer when device is attached” is checked.

Tap **OK** to return to the Control Panel. If desired, any control panel windows may be closed.

Select **Start > Settings > Scanner** and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

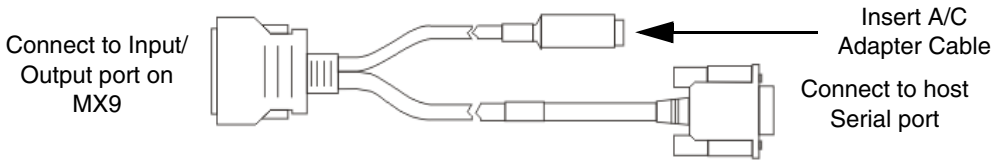
Connect the correct cable to the PC (the host) and the mobile device (the client). Select “Connect” from the Start Menu on the client (**Start > Programs > Communications > Connect**).

Note: Run “Connect” when the “Get Connected” wizard on the host PC is checking COM ports to establish a connection for the first time.

Cable for Serial ActiveSync Connection

MX9055CABLE - MX9 Serial Cable Assembly (ActiveSync connection)

- Connect the I/O connector to the I/O port on the bottom of the MX9.
- The serial port on the MX9 cable connects to a COM port on a PC or laptop.
- It is not necessary to connect the power receptacle to the MX9 power adapter in order to use ActiveSync. Do not allow the MX9 to enter Suspend while connected.



Wireless Connection

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using direct serial or USB cable connection.

Once the relationship is established using the USB or serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is Network.

Select **Start > Settings > Programs > Communication > ActiveSync**. From the popup list, choose Network and then tap the Connect button.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

To initiate synchronization from your MX9, tap **Start > Programs > Communication > ActiveSync** to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start > Help** for context-sensitive help.

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a host PC using the appropriate cables and Microsoft's ActiveSync or Windows Mobile Device Center.

Prerequisite

A partnership between the MX9 and ActiveSync has been established.

Serial Port Transfer

- A host PC with an available serial port and a MX9 with a serial port. The host PC must be running Windows.
- Null modem cable with all control lines connected. Use the specific serial cable shown in *Cable for Serial ActiveSync Connection*.

USB Transfer

- A host PC with an available USB port and a MX9 with a USB port. The host PC must be running Windows.
- Use the specific USB cable as show in *Cable for USB ActiveSync Connection*.

Connect

1. Connect the modem cable to the PC (the host) and the MX9 (the client).
2. Select "Connect" from the Start Menu on the mobile device (**Start > Programs > Communications > Connect**).
3. Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

USB synchronization will start automatically when the cable is connected, not requiring you to select "Connect" from the Start menu.

Disconnect

Depending on the type of connection, follow the instructions below to disconnect the MX9 from the host and close ActiveSync.

USB Connection

1. Disconnect the cable from the MX9.
2. Tap the status bar icon in the lower right hand corner of the status bar.
3. Tap the Disconnect button.

IMPORTANT – DO NOT PUT THE MX9 IN SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Serial Connection

1. Disconnect the cable from the MX9.
2. Put the mobile device into Suspend.
3. Tap the status bar icon in the lower right hand corner of the status bar.
4. Tap the Disconnect button.

Network Connection

1. Put the MX9 into Suspend.
2. Tap the status bar icon in the lower right hand corner of the status bar.
3. Tap the Disconnect button.

ActiveSync Help

Issue:

ActiveSync on the host says that a device is trying to connect, but it cannot identify it.

Solution:

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the MX9 is connected to a PC by a cable, disconnect the cable from the MX9 and reconnect it again.

Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

See Also: “Cold Boot and Loss of Host Reconnection”.

Issue:

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

Solution:

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

Issue:

ActiveSync indicator on the host turns green and spins, but connection never occurs.

Solution:

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

Issue:

ActiveSync indicator on the host remains gray.

Solutions:

Solution 1: ActiveSync icon on the PC does not turn green after connecting USB cable from MX9.

1. Disconnect MX9 USB cable from PC.
2. Suspend/Resume or Restart the MX9.
3. In **ActiveSync > File > Connection Settings** on PC disable Allow USB Connections and tap **OK**.
4. Re-enable Allow USB Connections on the PC and tap **OK**.
5. Reconnect USB cable from MX9 to PC.

Solution 2: The host doesn’t know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (**Control Panel > System > Device Name**)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

Configuring the MX9 with HSM Connect (or LXEConnect)

HSM Connect allows a user to view the MX9 screen remotely from a host PC using an ActiveSync connection:

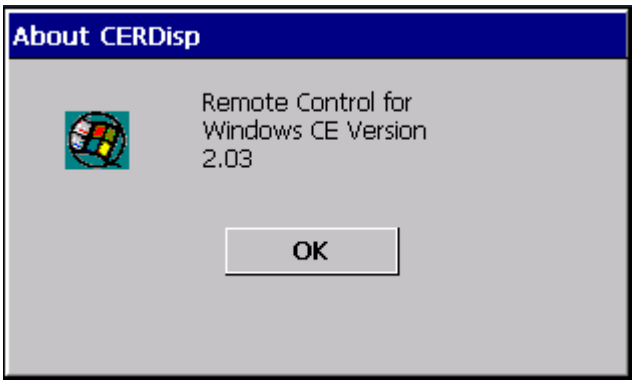
- ActiveSync is already installed on the MX9. The MX9 is preconfigured to establish a USB ActiveSync connection to a host PC when the MX9 USB/Power cable connects the MX9 and the host PC.
- If the MX9 uses a serial port for ActiveSync, it will be necessary to configure the MX9 to use the serial port. Complete details on the proper cables and port configuration are included in Initial Setup (page 5-72).

Installing HSM Connect (or LXEConnect)

1. Contact Technical Assistance for the HSM Connect files.
2. Download the files to a location on your host computer hard drive.
3. Run the setup.exe file that was copied to the host computer. The setup program installs the HSM Connect utility on the host computer.
4. Follow the on screen installation prompts.
5. When the installation is complete, create a desktop shortcut.
6. HSM Connect (or LXEConnect) is now installed on the host computer and ready to use.

Using HSM Connect (or LXEConnect)

1. Power up the MX9.
2. Connect the MX9 to the host computer using the USB/Power or Serial/Power cable. Once connected, the ActiveSync dialog box appears and the ActiveSync connection is automatically established.
3. Select **No** for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use HSM Connect. However if a partnership is desired for other reasons, one may be established now.
4. Double-click the HSM Connect icon you created on the host PC desktop.
5. HSM Connect launches.



6. Click the **OK** button to dismiss the About CERDisp dialog box on the MX9 desktop by clicking the OK button in the HSM Connect window on the host PC desktop. The dialog box automatically times out and disappears after approximately 20 seconds.

7. The host PC displays the MX9 screen.



8. The MX9 can now be configured from the HSM Connect window. Input from the host PC's mouse and keyboard are recognized as if they were attached to the MX9.

9. When the remote session is complete, close the HSM Connect program by selecting **File > Exit** or clicking on the **X** in the upper right hand corner to close the application on the host PC, then disconnect the ActiveSync cable.

Note: After using HSM Connect, the MX9 cannot go into Suspend mode until after a warmboot. If using Power Management on a MX9, always warmboot the MX9 when finished using HSM Connect.

6 AppLock

Introduction

Start > Settings > Control Panel > Administration

AppLock (application Locking) is designed to be run on Windows based devices only. The AppLock program is installed before shipping.

Configuration parameters are specified by the AppLock Administrator for the MX9 end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the MX9 boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this chapter, is that the first user to power up a new mobile device is the system administrator.

MX9 AppLock is setup by the Administrator by tapping **Start > Settings > Control Panel > Administration**.

Note: AppLock Administrator panel file Launch option does not inter-relate with similarly-named options contained in other System Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

Setup a New Device

Prerequisites:

- An MX9 default input method (Input Panel, Transcriber, or custom input method) is assigned.
- The touch panel must be enabled. Refer to the MX9WM Options control panel Touch Screen Disable setting. If the Touch Screen Disable option is dimmed, the touch panel cannot be turned on or off.

Devices with AppLock are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the MX9 and no password prompt is displayed. After the administrator specifies applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the MX9 switches to end-user mode.

The process to configure a new device is as follows:

1. Insert a fully charged battery and press the Power button.
2. Connect an external power source to the device (if required).
3. Adjust screen display, audio volume and other parameters if desired. Install accessories (e.g., handstrap, stylus).
4. Tap Start and open the Administration control panel.
5. Assign a Switch Key (hotkey) sequence for AppLock on the Security Panel.
6. Assign an application on the Application panel. More than one application can be assigned.
7. Assign a password on the Security panel.
8. Select a view level on the Status Panel, if desired.
9. Tap **OK**.
10. Press the Switch Key sequence to launch AppLock and lock the configured application(s). The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

- Administrator Hotkey - Shift+Ctrl+A
- User Activation Hotkey - Ctrl+Spc
- Password - none
- Application path and name - none
- Application command line - none

End User Mode

The default end user Hotkey Activation key is Ctrl+Spc.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows OS key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows OS desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three attempts) to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These situations include:

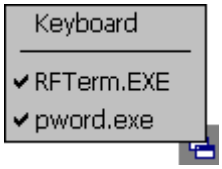
- If inaccurate configuration information is entered by the administrator, i.e., an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g., missing DLLs).
- Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

AppLock Password Help

Contact Technical Assistance (page 15-1) for help when troubleshooting passwords.

End-User Switching Technique



A checkmark in the switchpad menu (see image above) indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX9 default input method (Input Panel, Transcriber, or custom input method) is activated.

The check to the left of the application name indicates that the application is active.

If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by tapping on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter.

When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

Hotkey (Activation hotkey)

If the mobile device uses AppLock to allow the user to switch between applications, the default Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet check box in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet check box is enabled, the Menu and Status check boxes are available.

Enabling the Menu check box displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu check box is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status check box is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE (or equivalent) should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet check box.

Application Configuration

The default Administrator Hotkey sequence is Shift+Ctrl+A.

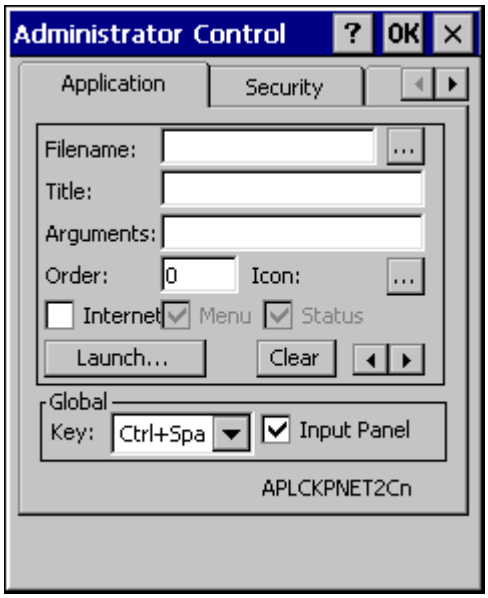
Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Panel.

If a password has not been configured, the Administrator panel is displayed.

Important: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application Panel



Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

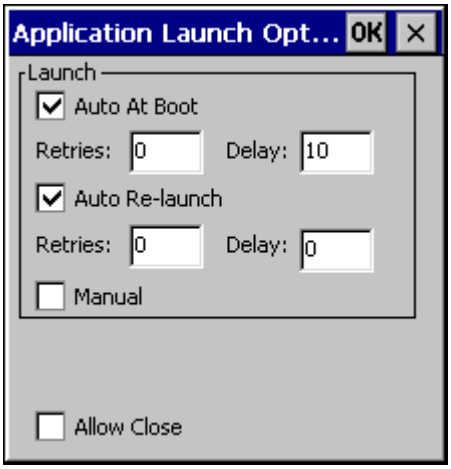
If no application is specified when the Administrator Panel is closed, the MX9 reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows Browse dialog is displayed. After selecting the application from the Browse dialog, tap **OK**.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.

Option	Explanation
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End User Internet Explorer (EUIE) (page 6-4)for more details.
Launch Button	See following section titled Launch Button (page 6-7).
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

When the Launch button is clicked, it displays the Launch options panel for the Filename selected on the Administration panel.



Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot

Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch

Default is Enabled.

When enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)

Default is Disabled.

Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a check mark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A check mark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Match

Default is blank (Match is not used).

AppLock works by associating display windows with the launched process ID. If an application uses different process IDs for windows it creates, the Match field must be used.

Use the Match field to specify up to 32 characters of the class name for the application.

- DOS applications using a standard DOS display box should specify condev_appcls in the Match text box.
- Remote Desktop (remote.exe) should specify TSSHELLWND in the Match text box.

Allow Close

Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Security Panel



Setting an Activation Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is Shift+Ctrl+A.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hot-key sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with <Shift>, <Alt>, and <Ctrl> text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the Soft Input Panel (SIP) are not guaranteed to work properly when switching operational modes.

For example, if the <Ctrl> key is pressed followed by <A>, Ctrl+A is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

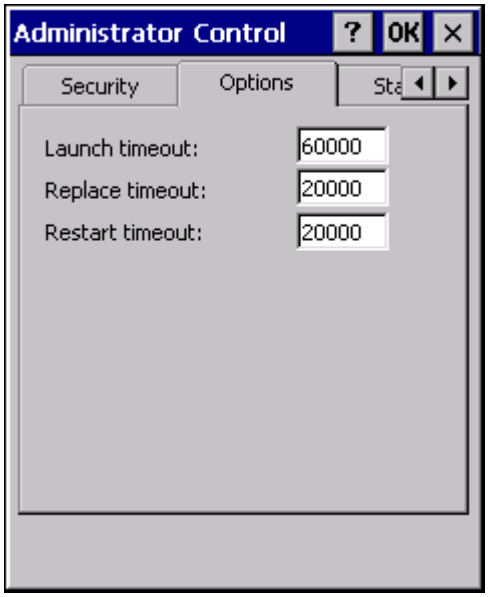
A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch user modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Setting a Password in the Security Panel

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

Options Panel



AppLock uses 3 timeout values when locking applications:

Launch timeout -- the time to wait for an application to initially launch before timing out. Default value is 60000 milliseconds (60 seconds).

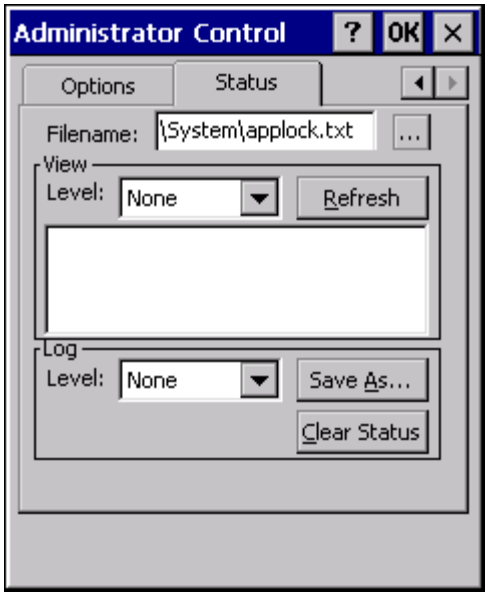
Replace timeout -- the time to wait for an application to replace the current window with another one before timing out. Default value is 20000 milliseconds (20 seconds).

Restart timeout -- the time to wait for an application to restart itself before timing out. Default value is 20000 milliseconds (20 seconds).

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the … button). The standard Windows OS Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap **OK**.

View

Select a View level from the drop down box. Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Error

Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.

Process

Processing status shows the flow control of AppLock components and is mainly intended for Customer Support when helping users troubleshoot problems with their AppLock program.

Extended

Extended status provides more detailed information than that logged by Process Logging.

All

All messages are displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

AppLock Help

Issue:

The MX9 won't switch from Administration mode to end-user mode.

Solution:

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Word and RFTerm, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

Issue:

The hotkey sequence needed is not allowed. What does this mean?

Solution:

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. Honeywell has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Issue:

Can't locate the password that has been set by the administrator?

Solution:

Contact Technical Assistance (page 15-1) for administrator password help.

AppLock Error Messages

Any messages whose first word ends in 'ing' is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	**Explanation and/or corrective action**	**Level**
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX

Message	Explanation and/or corrective action	Level
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX

Message	Explanation and/or corrective action	Level
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX

Message	Explanation and/or corrective action	Level
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

7 Bluetooth Configuration

Introduction

Start > Settings > Control Panel > Bluetooth

Discover and manage pairing with nearby Bluetooth devices.

Contact Technical Assistance (page 15-1) for upgrade availability if your Bluetooth panels are not the same as the panels presented in this section.

Setting	Default
Discovered Devices	None
Settings	
Bluetooth button (Toggle client On/Off)	Bluetooth client is On.
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printer Port on COM9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	System Device Name
Reconnect	
Report lost connection	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled
OPP Setup	
Inbox	\My Device\My Documents\DefaultInbox
Outbox	\My Device\My Documents\DefaultOutbox
Write Capable	Enabled
Enable Notifications	Enabled
Disable EZPair OPP	Unchecked, OPP is enabled

Bluetooth icon (at the bottom of the Today or desktop panel) state and Bluetooth device icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the MX9.

- The MX9 cannot be discovered by other Bluetooth devices when the **Computer is discoverable** option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- When Filtered Mode is enabled, the MX9 can pair with one Bluetooth scanner and one Bluetooth printer.
- When Filtered Mode is disabled, the MX9 can pair with up to four Bluetooth devices, with a limit of one scanner, one printer, two HID devices (one Mouse, one Keyboard), one PAN device, and one DUN device connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the MX9.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the MX9 during the pairing process.

Assumptions:

- The System Administrator has Discovered and Paired targeted Bluetooth devices for the MX9.
- The MX9 operating system has been upgraded to the revision level required for Bluetooth client operation.
- An application (or API) is available that will accept data from serial Bluetooth devices.

HID	Human Interface Device	HID profiles used by Bluetooth keyboards, mice, pointing devices and remote monitoring devices.
PAN	Personal Area Networking	PAN profiles, unmodified Ethernet payloads (using BNEP) can exchange packets between Bluetooth devices. PANU is a PAN User service that uses either the NAP or the GN service.
DUN	Dial-Up Networking	DUN provides access to the Internet and other dial-up services using Bluetooth technology.

Initial Configuration

1. Open the Bluetooth control panel or tap the Bluetooth icon.
2. Tap the Settings Tab.
3. Change the Computer Friendly Name at the bottom of the Settings panel. The Bluetooth MX9 default name is determined by the factory installed software version. Honeywell strongly urges assigning every MX9 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the MX9 Bluetooth options on the Settings tab and the Reconnect tab.
5. Tap the OK button to save your changes.

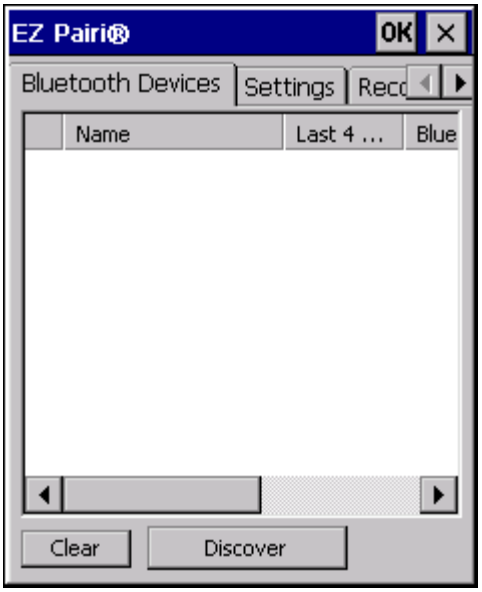
Subsequent Use

Note: Bluetooth client icon and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. A Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

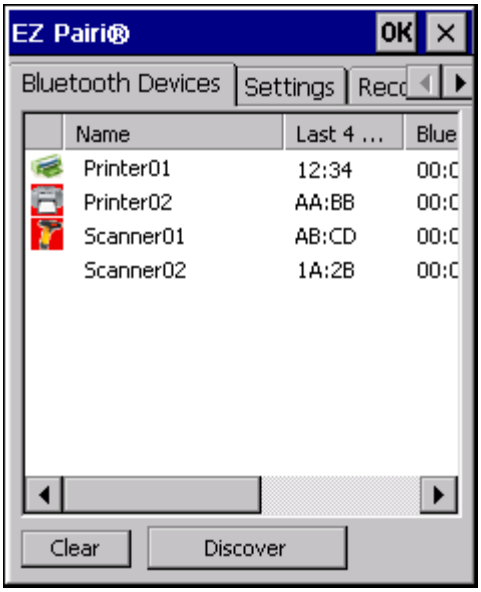
1. Tap the Bluetooth client icon to open the Bluetooth EZPair (or LXEZ Pairing) application.
2. Tap the Bluetooth Devices tab.
3. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap Pair as Scanner to set up the MX9 to receive scanner data.
7. Tap Pair as Printer to set up the MX9 to send data to the printer.
8. Tap Serial Device (when Filtered mode is disabled) to set up the MX9 to communicate with a Bluetooth serial device.
9. Tap HID Device to pair a HID device.
10. Tap PAN Device to pair a PAN device.
11. Tap DUN Device to pair a DUN device.
12. Tap Disconnect to stop pairing with the device. Once disconnected, tap Clear to remove the device name and data from the MX9 Bluetooth Devices list. Select Yes at the "Delete *all disconnected devices? Yes / No*" dialog box.
13. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX9 display.
14. Whenever the MX9 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the MX9. If the devices cannot connect to the MX9 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if *Report Failure to Reconnect* is disabled.

Bluetooth Devices

The Bluetooth Devices tab displays any device previously discovered and paired with the MX9.



Before Discover



After Discover

Clear Button

When the Clear button is tapped, the Bluetooth client deletes all devices from the Device table that are not currently paired. A dialog box is presented stating *Delete all disconnected devices?*

Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence and when EZPair (or LXEZ Pairing) is re-launched without rebooting. Tap the No button to make no changes.

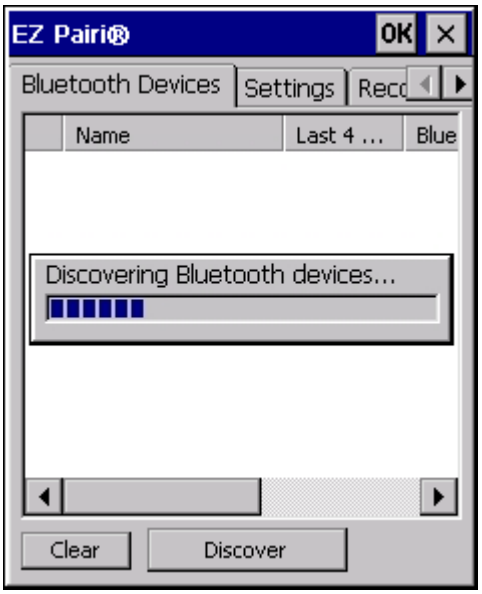
Discover Button

When the Discover button is tapped, the Bluetooth client discovers and displays all Bluetooth devices in the vicinity. Bluetooth managed devices should be as close as possible, in direct line of sight, with the MX9 during the Discover process.

At the end of the Discover process, and when Filtered Mode is disabled (not checked), serial Bluetooth devices as well as Bluetooth scanners and printers are displayed in the Device table. When Filtered Mode is enabled (checked), only Bluetooth scanners and printers are displayed in the Device table.

Discovering

1. Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.



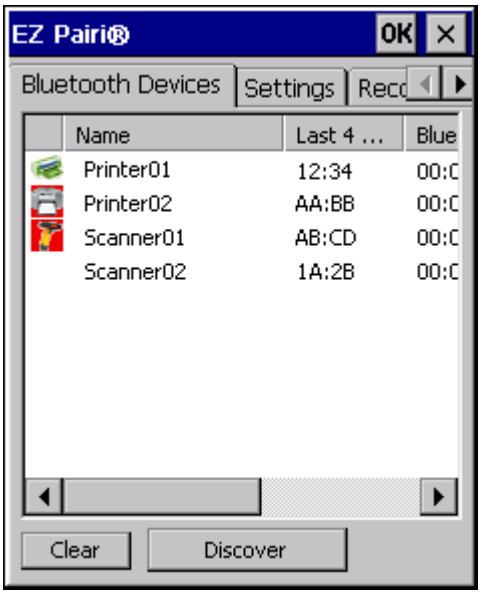
2. Tap Stop at any time to end the Discover and Query for Unique Identifier functions.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX9 Bluetooth scanning range, the Bluetooth connection between the paired device and the MX9 is lost. There may be audible or visual signals as paired devices disconnect from the MX9.

Stop Button

Tap Stop at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after any reboot sequence.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Serial device, Scanner, or a Printer. The Bluetooth panel assigns an icon to the device name.

An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the MX9 and the device's Bluetooth connection is active.

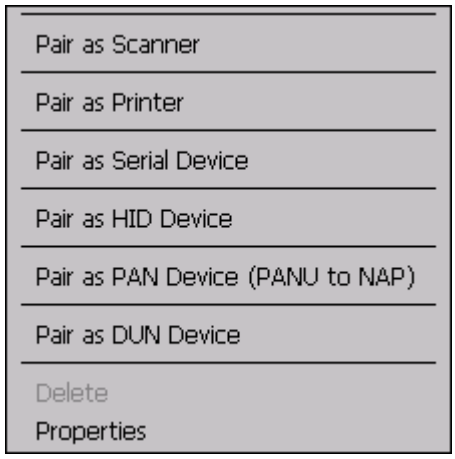
Double-tap a device in the list to open the device properties menu. The opened device does not need to be active.

Bluetooth Device Menu

1. After the Discover button has been tapped and there are devices listed, tap on a device in the list to highlight it.
2. Double-tap the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.



Filtered Mode on



Filtered Mode off

Right Click Menu Options

Pair as Scanner

Receive data from the highlighted Bluetooth scanner or Bluetooth imager.

Pair as Printer

Send data to the highlighted Bluetooth printer.

Pair as Serial Device

Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled/unchecked.

Pair as HID device

Communicate with the highlighted HID (Human Interface Device). This option is available when Filtered Mode is disabled/unchecked.

Pair as PAN Device (PANU to NAP)

Communicate with the highlighted PAN (Personal Area Networking) device. This option is available when Filtered Mode is disabled/unchecked.

Pair as DUN Device

Communicate with the highlighted DUN (Dial-Up Networking) device. This option is available when Filtered Mode is disabled/unchecked.

Disconnect

Stop the connection between the MX9 and the highlighted paired Bluetooth device.

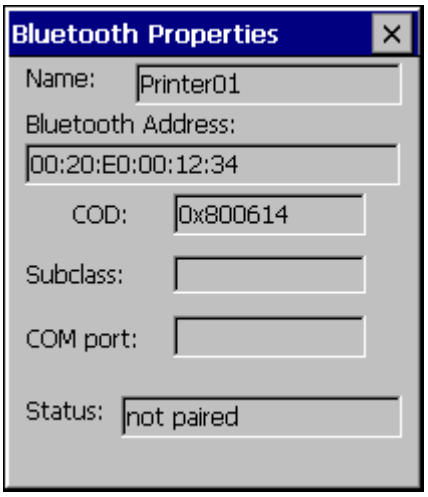
Delete

Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the MX9 Bluetooth Devices panel when the user taps the Clear button.

Properties

View more information on the highlighted Bluetooth device.

Bluetooth Properties

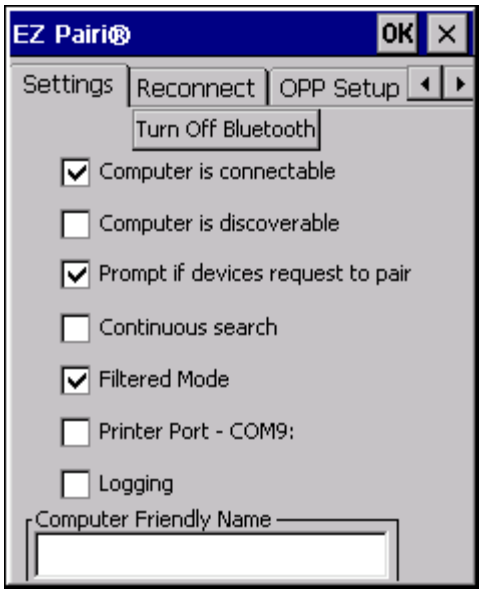


Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings

Note: Options can be checked or unchecked whether Bluetooth connection is enabled or disabled.



Turn On Bluetooth (Button)

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn On Bluetooth* to *Turn Off Bluetooth*.

The default value is Enabled (Bluetooth client is On).

Options

Computer is connectable

This option is Enabled (checked) by default. Disable this option to inhibit MX9 connection initiated by a Bluetooth scanner.

Computer is discoverable

This option is Disabled (unchecked) by default. Enable this option to ensure other devices can discover the MX9.

Prompt if devices request to pair

This option is Enabled (checked) by default. A dialog box appears on the MX9 screen notifying the user a Bluetooth device requests to pair with the MX9. The requesting Bluetooth device does not need to have been Discovered by the MX9 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.

Continuous Search

This option is Disabled (unchecked) by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the MX9 stops searching after 30 minutes.

Note: Continuous Search option continually draws power from the Main Battery until timeout.

Filtered Mode

This option is Enabled (checked) by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the MX9 can pair with up to four Bluetooth devices, with a limit of one Bluetooth scanner, one Bluetooth printer, one PAN, and one DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. A Registry/Restart is required every time Filtered Mode is toggled on and off.

Printer Port - COM9

This option is Disabled (unchecked) by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled/checked.

Logging

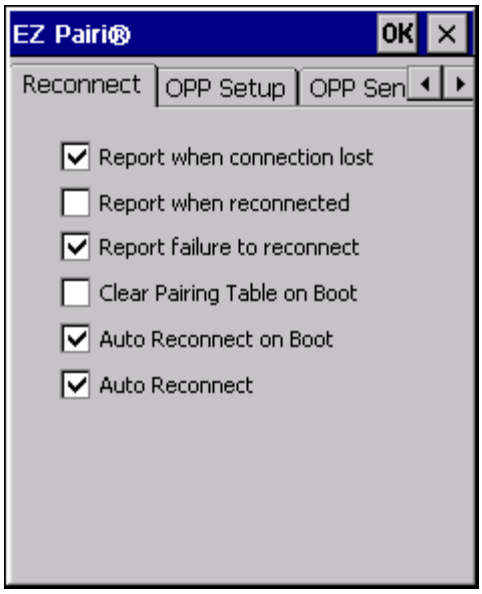
This option is Disabled (unchecked) by default. When logging is enabled, the MX9 creates bt_log.txt and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A bt_log_bak.txt file contains the data stored by bt_log.txt prior to reboot. During a reboot process, the MX9 renames bt_log.txt to bt_log_bak.txt. If a file already exists with that name, the existing file is deleted, the new bt_log_bak.txt file is added and a new bt_log.txt is created.

Computer Friendly Name

This option is populated with the [*System Name*] when EZ Pair is installed. The System Administrator can change the name. The Computer Friendly Name entered in this space is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.



Options

Report when connection lost

This option is Enabled by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.

Report when reconnected

This option is Disabled by default. There may be an audio or visual signal when a connection between a paired, active device is made. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the ok button to remove the dialog box from the screen.

Report failure to reconnect

This option is Enabled by default. The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. Tap the X button or ok button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.

Clear Pairing Table on Boot

This option is Disabled by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) “Auto Reconnect on Boot” is automatically disabled (dimmed).

Auto Reconnect on Boot

This option is Enabled by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.

Auto Reconnect

This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior. When Auto Reconnect is disabled (unchecked), Auto Reconnect on Boot is automatically disabled and dimmed. When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of Auto Reconnect on Boot is ignored and no devices are reconnected on boot. The status of Clear Pairing Table on Boot controls whether the pairing table is populated on boot. When Auto Reconnect is enabled (checked) and Auto Reconnect on Boot is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). When Auto Reconnect is enabled (checked) and Clear Pairing Table on Boot is enabled (checked), devices are not

reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of Auto Reconnect on Boot is ignored and the option is automatically disabled (unchecked) and dimmed.

See Using OPP (page 7-15) for instruction for the *OPP Setup* and *OPP Send* panels.

About

This panel shows the Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth Client MAC address, and software version levels. The data cannot be edited by the user.



Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range.

Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the MX9 while AppLock is in control.

Bluetooth Indicators

The Bluetooth icon state and Bluetooth LED state change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the MX9.

Taskbar Icon	Legend
	MX9 is connected to one or more of the targeted Bluetooth device(s).
	MX9 is not connected to any Bluetooth device. MX9 is ready to connect with any Bluetooth device. MX9 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX9 Bluetooth scan range, the Bluetooth connection between the paired device and the MX9 is lost. There may be audible or visual signals as paired devices disconnect from the MX9.

MX9 Bluetooth LED	Legend
Blue, blinking slowly	Bluetooth is active but not connected to a device.
Blue, blinking medium	Bluetooth is paired and connected to a device.
Blue, blinking fast	Bluetooth is discovering other Bluetooth devices.
Off	Bluetooth hardware has been turned off or does not exist in the MX9.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the MX9 while AppLock is in control.

Bluetooth Bar Code Reader Setup

Refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance (page 15-1) for Bluetooth product assistance.

Introduction

Honeywell supports several different types of bar code readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the MX9 using Bluetooth functions.

Prerequisites

- The MX9 must have the Bluetooth hardware and software installed. An operating system upgrade may be required.
- If the MX9 has a Bluetooth address identifier bar code label affixed, then Bluetooth hardware and software are installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The MX9 main battery is fully charged. Alternatively, the MX9 may be cabled to AC/DC power.
- **Important:** The bar code numbering examples in this segment are not real and should not be created or scanned with a Bluetooth scanner.
- Open the Bluetooth control panel or tap the Bluetooth icon.

LnkB00440fd01020 - Sample



Locate the bar code label, similar to the sample shown above, attached to the MX9. The label is the Bluetooth address identifier for the MX9.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

The MX9 Bluetooth address identifier label should be protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth bar code readers.

MX9 with Label

If the MX9 has a Bluetooth address bar code label, follow these steps:

1. Scan the Bluetooth address bar code label, attached to the MX9, with the Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the MX9 Bluetooth label, the devices are paired. See Bluetooth Reader Beep and LED Indications (page 7-14). If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel (**Start > Settings > Control Panel > Bluetooth**).
4. Tap Discover. Locate the Bluetooth scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth scanner. The right-mouse-click menu appears.
6. Select Pair as Scanner to pair the MX9 with the Bluetooth mobile scanner.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and an LED flashes.

Note: After scanning the MX9 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

MX9 without Label

If the Bluetooth address bar code label does not exist, follow these steps to create a unique Bluetooth address bar code for the MX9:

1. First, locate the MX9 Bluetooth client MAC address by opening the About tab.
2. Next, create a Bluetooth address bar code label for the MX9. Free bar code creation software is available for download on the World Wide Web. Search using the keywords *bar code create*.
3. The format for the bar code label is as follows:
   - Bar code type must be Code 128.
   - FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.
4. Create and print the label.
5. Scan the MX9 Bluetooth address bar code label with the Bluetooth bar code reader.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes.

Note: After scanning the MX9 Bluetooth label, if there is no beep and no LED flash from the remote Bluetooth device, the devices are currently paired.

Bluetooth Reader Beep and LED Indications

Bluetooth Remote Device Beep Type

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

Bluetooth Remote Device LED

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the remote Bluetooth scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact Technical Assistance (page 15-1) for help.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible (no more than 32.80 feet [10 meters] line of sight in a quiet environment) to the MX9 during the pairing process.

1. Open the Bluetooth control panel.
2. Tap Discover. Locate the remote Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or double-tap) on the Bluetooth printer until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the MX9 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Refer to the remote Bluetooth printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance (page 15-1) for Bluetooth product help.

Note: If there is no beep or no LED flash from the remote Bluetooth printer, the MX9 and the printer are currently paired.

Using OPP

Pairing with an OPP Device

Prerequisites

- A remote device, such as a mobile phone, that supports OPP.
- OPP is enabled on the MX9.

1. Place the remote device in discovery or visible mode.
2. Initiate discovery on the MX9 by tapping the Discover button on the OPP Send tab.
3. The MX9 discovers the remote device.
4. The MX9 attempts to send a file to the remote device.
5. The remote device prompts the user for a 4 digit PIN.
6. User enters the PIN.
7. The MX9 prompts the user for a 4 digit PIN.
8. User must enter the same PIN code as entered on the remote device.
9. The MX9 now pairs with the remote device.

Remote Device Pushes File to MX9

This section assumes that a device supporting OPP is paired with the MX9.

If a duplicate filename is received, EZPair (or LXEZ Pairing) writes the file in the specified location, with an incremental number appended to the file name. For example, if a file named file.jpg is pushed to the MX9 and that filename already exists in the Inbox, EZPair saves the new file as file001.jpg. If the same file is pushed again, it is saved as file002.jpg.

Following are several scenarios based on configuration options on the OPP Setup tab.

Notifications enabled, MX9 is Write Capable

1. The OPP client initiates a connection to the MX9 by selecting a file to push to the MX9.
2. The MX9 user is notified that a File Push request has been issued from a remote device.
3. The MX9 user is prompted to accept or reject the incoming request.
4. If the user accepts the request:
    - The file is pushed to the MX9.
    - EZPair notifies the user that a file has been received.
    - The connection is closed by the remote device (OPP client).
5. If the user rejects the request:
    - The file is not pushed to the MX9.
    - The connection is closed.

Notifications enabled, MX9 is not Write Capable

1. The OPP client initiates a connection to the MX9 by selecting a file to push to the MX9.
2. The file is rejected silently (no notification to the MX9 user).

Notifications disabled, MX9 is Write Capable

1. The OPP client initiates a connection to the MX9 by selecting a file to push to the MX9.
2. The file is accepted silently (no notification to the MX9 user).

Notifications disabled, MX9 is not Write Capable

1. The OPP client initiates a connection to the MX9 by selecting a file to push to the MX9.
2. The file is rejected silently (no notification to the MX9 user).

MX9 Pushes File to Remote Device

This section assumes that a device supporting OPP is paired with the MX9.

The MX9 (OPP client) initiates a connection to the remote device (OPP server) by selecting a file to push to the remote device. The MX9 sends the file and disconnects. The remote device may prompt the user (of that remote device) to accept the incoming request depending on the security settings of the remote device. The prompt may be displayed more than once, or it may not be displayed at all.

Notifications enabled

The file is pushed to the remote device and the user of the MX9 is notified of the completion of the push.

Notifications disabled

The file is pushed to the remote device and the user of the MX9 is not notified of the completion of the push.

EZPair (or LXEZ Pairing) and External Applications

Because only one application can use the OPP service at a time, external applications that wish to use OPP should disable EZPair OPP before using the OPP service and restore EZPair OPP upon completion using available API calls (see the *CE API Programming Guide* for details). These API calls are the equivalent of checking or unchecking the Disable EZPair OPP checkbox.

- If Disable EZPair OPP is not checked, checking it causes EZPair OPP to be disabled and the send and receive functionality is disabled.
- If Disable EZPair OPP is checked, and no application has registered a callback, un-checking EZPair OPP enables OPP functionality in EZPair, and the send and receive functionality is enabled.
- If Disable EZPair OPP is checked, and another application has registered a callback, un-checking Disable EZPair OPP issues a dialog box which says “Another application is using OPP. Do you wish to force their disconnection? Doing so will force the other application to be unregistered.” The application that has been forcibly unregistered receives a FORCED_UNREGISTER_RECEIVED event.

OPP Setup Tab

Use this screen to setup the MX9 for Object Push Protocol (OPP).



Inbox

This is an alphanumeric field displaying the currently selected Inbox.

- The Inbox is the location where files pushed to the MX9 from a remote client are stored. Use the browse button ... to browse to and select the Inbox folder.
- Use Windows Explorer to create a custom directory, if desired, before selecting the Inbox folder.

The default Inbox is \My Device\My Documents\DefaultInbox.

Outbox

This is an alphanumeric field displaying the currently selected Outbox.

- The Outbox is the location where files are stored to be pushed from the MX9 to a remote server. Use the browse button ... to browse to and select the Outbox folder.
- Use Windows Explorer to create a custom directory, if desired, before selecting the Outbox folder.

The default Inbox is \My Device\My Documents\DefaultOutbox.

Write Capable

When checked, files may be written to the MX9. When unchecked, inbound files are rejected.

This option is enabled (checked) by default.

Enable Notifications

When checked, the user is notified and may be prompted for a response when files are received by the MX9. When unchecked, inbound files are received with no notification to and no required action from the user.

This option is enabled (checked) by default.

Disable EZPair (or LXEZ Pairing) OPP

When checked, OPP is disabled in EZPair (or LXEZ Pairing). When unchecked, OPP is enabled in EZPair (or LXEZ Pairing).

The default is unchecked, OPP is enabled for EZPair (or LXEZ Pairing).

- Because only one application can use OPP at a given time, custom applications should disable OPP in EZPair (or LXEZ Pairing) via an API call while the application is using OPP and restore this setting upon completion.
- When this item is checked, the other parameter settings on this screen are unavailable (dimmed).

OPP Send Tab



When EZPair OPP is disabled, no file names or OPP servers are displayed on this tab. These areas are grayed out. Similarly the buttons on this tab are also inactive when EZPair OPP is disabled.

Send Selected File From Outbox

This area displays the file listing from the currently selected Outbox. All files are shown (*.*). The most recently pushed file is highlighted, assuming the file is still present in the Outbox.

Select OPP Server from Remote Device List

This list displays the known OPP capable servers that the MX9 has previously discovered. The most recently paired server is selected and highlighted.

Buttons

Send - Tapping this button sends (pushes) the selected file to the remote (server) device.

Cancel - Tapping this button cancels the send process initiated by tapping the Send button.

Discover - Tapping this button initiates a discovery of OPP devices. Results of the discovery are shown in the OPP Server selection box.

8 Data Collection Wedge

Introduction

Start > Settings > Control Panel > Data Collection

Set scanner/imager keyboard wedge parameters, enable or disable symbologies from being scanned, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Scanner parameters apply to the MX9 integrated scanner/imager only. Bar code manipulation parameters apply to bar codes scanned by the MX9 integrated scanner/imager engine.

Scanner configuration can be changed using the Data Collection settings panels or via API functions. While the changed configuration is being read, the Scanner LED is solid amber. The scanner is not operational during the configuration update.

The MX9 has one integrated bar code scanner/imager port. Only one scan engine is installed at a time. Scan engines are not “hot swappable”. The MX9 may have one of the following bar code scan engines:

- Symbol Short Range Laser Scanner, 955
- Symbol Multi-Range “LORAX” Laser, 1524ER
- Hand Held Products 2D Area Imager, 5300

The integrated scan engine activates when the Scan button on the front of the MX9 is depressed or when the trigger on an installed trigger handle is depressed.

Symbol scanner

Refer to the *Integrated Scanner Programming Guide* for instruction on configuring specific scanner/imager parameters by using the MX9 to scan engine-specific setup bar codes in the guide.

Hand Held Products (HHP) Imager

Use the HHP Properties button on the Data Options tab and the Advanced button available on many of the individual Symbology Settings screen to configure the Hand Held Products Imager. There are no configuration bar codes for this imager.

External Bar Code Readers

The MX9 can use the following external bar code readers:

- Tethered hand-held scanners are tethered to a serial port on the MX9 or cradle and are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.
- Wireless hand-held Bluetooth scanners are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.
- The body worn Bluetooth Ring Scanner module may be using a Symbol 4400 Ring Imager or a Symbol 955 Ring Scanner. The Bluetooth Ring Scanner module is configured by scanning the bar codes in the *Bluetooth Ring Scanner Programming Guide*.

Return to Factory Default Settings

After scanning the engine-specific bar code to return the scanner/imager to factory default settings, the next step is to open the bar code wedge panel on the mobile device collecting the scanned data. Click the OK button to close the panel. This action will synchronize all scanner formats for your device. Another option you can use to reset the Data Collection panel is to scan the LXEReset bar code (for Symbol and Hand Held Products scan engines) located in the *Integrated Scanner Programming Guide*.

Engine specific bar codes for integrated scanners are contained in the *Integrated Scanner Programming Guide.* They can be used to set or reset scan engine parameters by scanning a bar code, then saving the change. Symbol scan engines can be programmed using programming bar codes. Do not scan decoder engine configuration bar codes when Continuous Scan Mode (page 8-4) is on. Configuration bar codes do not decode when scanned while Continuous Scan Mode is On.

Data Processing Overview

Bar code data processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Symbology Settings panels. The steps are presented below in the order they are performed on the scanned data.

1. Scanned data is tested for a code ID and length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the bar code data is processed based on the settings for All.
2. If the symbology is disabled, the scan is rejected.
3. Strip leading data bytes unconditionally.
4. Strip trailing data bytes unconditionally.
5. Parse for, and strip if found, Data Options strings.
6. Replace any control characters with string, as configured.
7. Add prefix string to output buffer.
8. If Code ID is not stripped, add saved code ID from above to output buffer.
9. Add processed data string from above to output buffer.
10. Add suffix string to output buffer.
11. Add a terminating NUL to the output buffer, in case the data is processed as a string.
12. If key output is enabled, start the process to output keys. If control characters are encountered:
    - If Translate All is set, key is translated to CTRL + char, and output.
    - If Translate All is not set, and key has a valid VK code, key is output.
    - Otherwise, key is ignored (not output).
13. If key output is disabled, a windows message is broadcast to notify listening applications that data is available.

The manipulated data is ready to be read by applications.

Main Tab

The Data Collection Wedge supports up to three concurrent data collection devices. For example, the internal scanner could be used to collect data at the same time a Bluetooth scanner is paired and/or a serial device is attached to COM1. The MX9 must be in a desktop cradle to use a tethered scanner.

Setting	**Default**
Device 1	Disabled
Device 2	Internal
Device 3	Disabled
Keep Awake	Disabled
Output	Disabled
Send Key Messages	Enabled
Scan Mode - Continuous	Disabled
Scan Mode - Timeout between same symbol	1 second

Device 1 – Internal. Radio button allows scanner input/output on Device 1 (scan key or trigger).

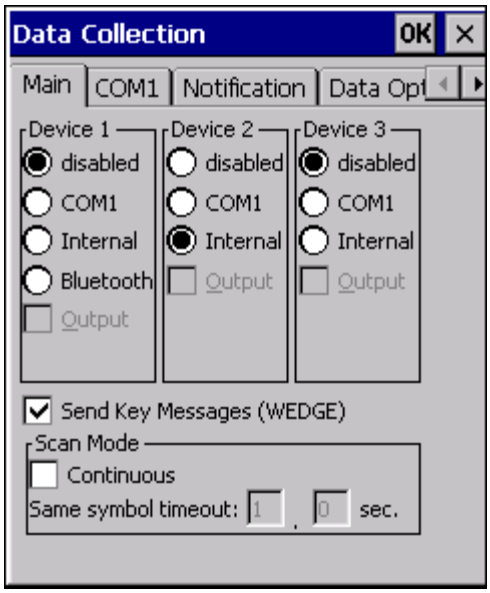
Device 2 – Output is enabled when COM1 is enabled on this port.

Device 3 – Output is enabled when COM1 is enabled on this port.

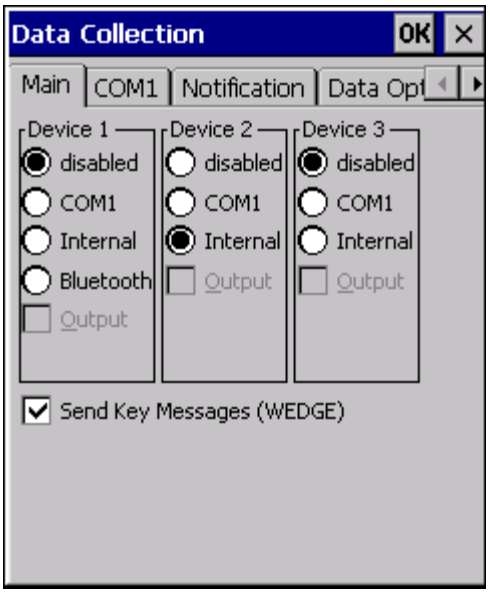
Note: Since Internal is the default setting for Device 2, a Bluetooth scanner can be paired with the Wedge on Device 1 without disabling the internal scanner.

Output – When Output is enabled, data is received from the scanner and processed via the wedge but an application can also open the WDG0: device and write data to it. An example is when a printer is connected to the same COM port as the scanner via a switch. Data can be written to the WDG device and is redirected to the associated COM port. The application must open the WDG0: port, not the COMx: port as the Wedge has exclusive rights to the COM port. If Output is not enabled, the WDG0: port can still be opened, but any attempts to write to that port fail.

Note: Adjust the settings and tap **OK** to save the changes. The changes take effect immediately.



Panel showing options for Symbol scan engine



Panel showing options for HHP scan engine

The Scan Mode (Continuous Scan) section is only present if the MX9 *is equipped with a Symbol integrated scanner.*

Continuous Scan Mode

Continuous scan mode is only available if the MX9 is equipped with a Symbol scanner. Continuous scan mode draws power from the main battery every time a scan read/decode sequence is performed.

Enabling Continuous Scan Mode will ensure the laser is always on and decoding.

Note: Do not scan decoder engine configuration bar codes when Continuous Scan Mode is on. Configuration bar codes do not decode when scanned while Continuous Scan Mode is On.



Caution: Laser beam is emitted continuously. Do not look or stare into the laser beam.

Set the Timeout between same symbol to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.

If trigger mode, power mode, or timeout between same symbol parameters are changed using external configuration bar codes in the *Integrated Scanner Programming Guide*, the operating system automatically restores the parameters to their programmed settings upon a cold boot and/or any change made in the Data Collection settings.

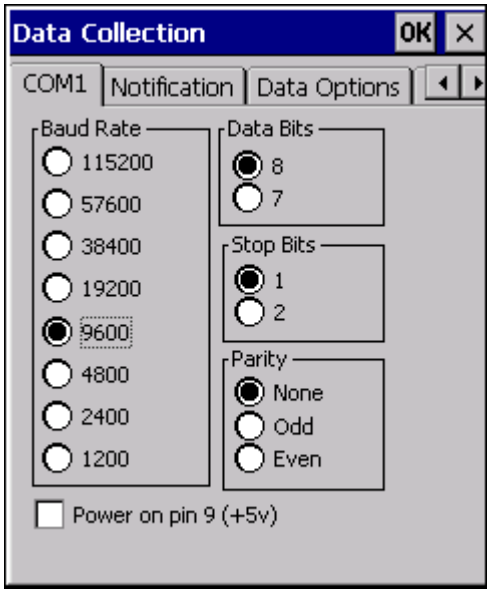
When the scanner is in continuous mode the trigger and scan buttons function as a scanner On/Off switch.

The scanner red LED will always be off in continuous mode. The audio beeps and green LED function the same as they do for normal trigger mode.

Switching to and from continuous and normal trigger modes is in effect after upon tapping the ok button and waiting for the amber scan LED to go out. A reboot is not required or necessary.

COM1 Tab

Setting	Default
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None



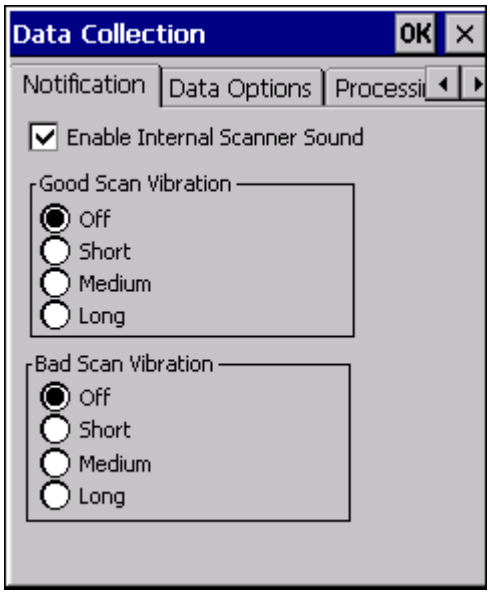
Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

If these values are changed, the default values are restored after a cold boot or reflashing.

Note: COM1 does not support 5V switchable power on Pin 9 for tethered scanners connected to the MX9 I/O port. Tethered scanners must be connected to a MX9 cradle.

Notification Tab

Setting	Default
Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Off
Bad Scan Vibration	Off



Internal Scanner Sound

This panel toggles internal scanner sounds on and off. Internal scanner sound, by default, is enabled.

Vibration

Vibration on the MX9 is activated when a scan is completed successfully or with a failure (scan key released before good scan, timeout, or rejected because of Data Options configuration). It is not activated when a trigger or scan key is pressed. The default setting for both Good Scan and Bad Scan vibration is Off.

Enable this parameter when a tactile response on a good scan or bad scan is desired. Scan sounds are accompanied by a tactile response when the internal scanner Sound parameter is enabled. Enable short, medium or long duration for each selection (good scan and bad scan).

When the MX9 does not have vibrate capability, any active vibration setting is ignored.

Data Options Tab

Bar code manipulation parameter settings on this tab are applied to the incoming data resulting from successful bar code scans sent to the MX9 for processing.

Note: The Data Options tab contains only those options available for one type of decoding engine.

Setting	**Default**
Enable Code ID	None
Symbology Settings	All
Control Character Translate All	Disabled
Custom IDs	Name blank
HHP Properties (Hand Held Products)	Options Disabled: Centering DecodeMode LinearRange AimTimer LeaveLightsOn

The Data Options tab contains several options to control bar code processing. Options include:

- Defining custom Code IDs.
- Disable processing of specified bar code symbologies.
- Rejecting bar code data that is too short or too long.
- Stripping characters including Code ID, leading or trailing characters and specified bar code data strings.
- Replacing control characters.
- Adding a prefix and a suffix.

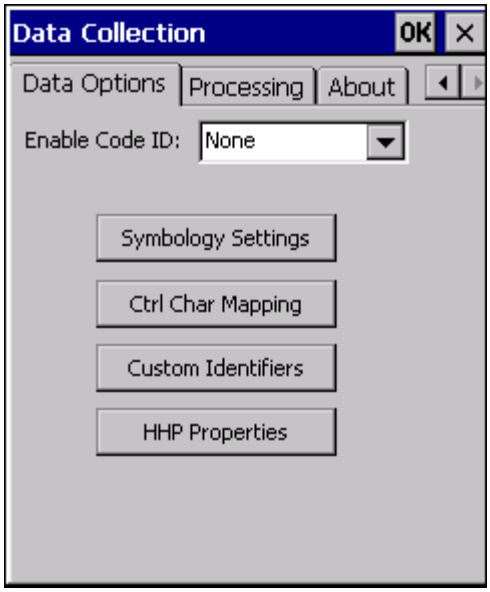
For MX9 with Symbol Decoding Engine

Data Collection Wedge can only enable or disable the *processing* of a bar code inside the Wedge software.

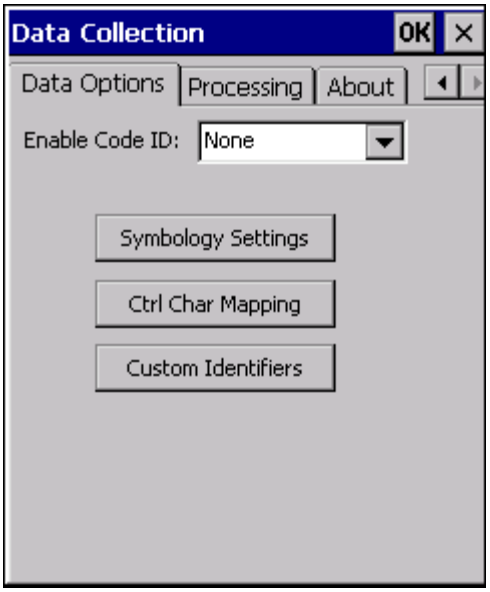
Enabling or disabling a specific bar code symbology at the scanner/imager is done manually using the configuration bar code in the *Integrated Scanner Programming Guide*.

For MX9 with Hand Held Products Decoding Engine

Data Collection Wedge enables or disables the bar code at the imager as well as enabling or disabling the bar code processing in the Wedge software.



Panel for a Hand Held Products scan engine



Panel for Symbol scan engine

The HHP Properties button is only present if the MX9 is equipped with a Hand Held products imager.

1. Choose an option in the Enable Code ID drop-down box:
   - None
   - AIM
   - Symbol
   - HHP
   - Custom
2. The Symbology screen is displayed.

Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of bar code identifier being processed. If the scanner being configured is not an integrated scanner, the scanner driver expects that the setting has been programmed into the scanner externally, and that the data will be coming in with the specified Code ID attached.

Transmission of the Code ID is enabled at the scanner for all bar code symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the bar code data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e., treated as a Code ID).
- UPC/EAN Codes only: The Code ID for supplemental bar codes is not stripped.
- When Enable Code ID is set to AIM, Symbol or HHP, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- Symbol equipped devices are configured using configuration bar codes, When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID ‘AAA’ is created to be read in combination with an AIM ID for Code 39 ‘]A1’, the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.

- The external scanner operation cannot be controlled by the MX9 scanner driver; therefore, a 'good' beep may be sounded from the external scanner even if a bar code from an external scanner is rejected because of the configuration specified. The MX9 will still generate a 'bad' scan beep, to indicate the bar code has been rejected.

Enable Code ID Options

None

Programs the internal scanner to disable transmission of a Code ID. The only entry in the Symbology popup list is All.

AIM

Programs the internal scanner to transmit the AIM ID with each bar code. The combo box in the Symbology panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.

Symbol

Programs the internal scanner to transmit the Symbol ID with each bar code. The combo box in the Symbology panel is loaded with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.

HHP

Programs the internal scanner to transmit the HHP ID with each bar code. The combo box in the Symbology panel is loaded with the known HHP ID symbologies for that platform, plus any custom Code IDs.

Custom

Does not change the scanner's Code ID transmission setting. The combo box in the Symbology panel is loaded with any configured Custom Code IDs.

Enable Code ID Buttons

Symbology Settings

Individually enable or disable a bar code from being scanned, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Barcode Data) add a prefix or suffix to a bar code before transmission.

Ctrl Char Mapping

Define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes.

Custom Identifiers

Defines an identifier that is at the beginning of bar code data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

HHP Properties

Set properties for a Hand Held Products imager including centering, mode, range, AIM timer and light behavior.
Note that the HHP Properties button is only present if the MX9 is equipped with a Hand Held Products imager.

Symbology Settings

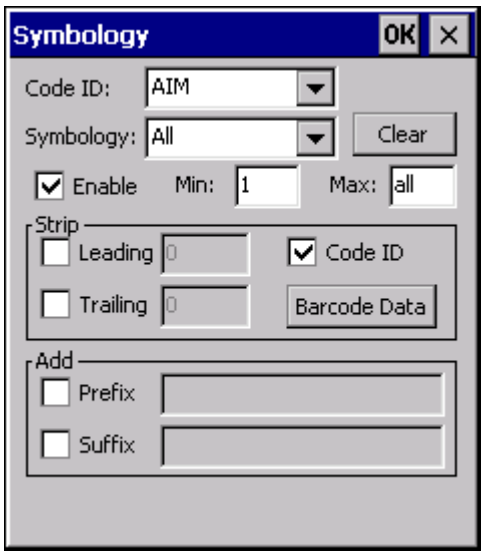
The Symbology selected in the Symbology drop down list defines the symbology for which the data is being configured. The features available on the Symbology panel include the ability to

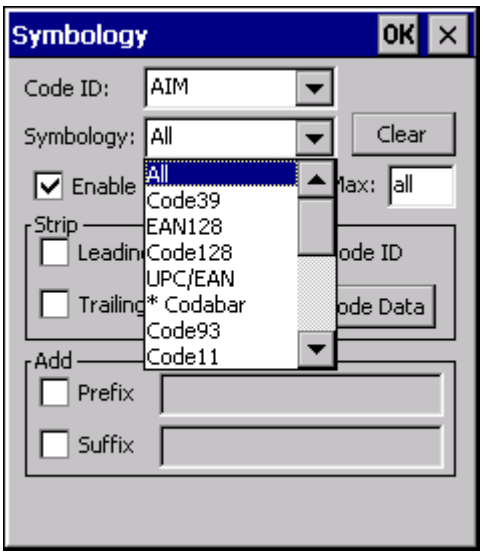
- individually enable or disable a bar code from scanning,
- set the minimum and maximum size bar code to accept,
- strip Code ID,
- strip data from the beginning or end of a bar code,
- or (based on configurable Barcode Data) add a prefix or suffix to a bar code.

The Code ID drop down box only filters the available symbologies in the Symbology drop down box by the selected Code ID. This Code ID box does not enable or disable the Code ID as that function is controlled by the Enable Code ID box on the Data Options tab.

The Symbology drop down box contains all symbologies supported by the device selected on the Main tab. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as ok is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop down list.





Clear Button

This button will erase any programmed overrides, returning to the default settings for the selected symbology.

If Clear is pressed when All is selected as the symbology, a confirmation dialog appears. Tap the Yes button and all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

Advanced Button

If there are advanced configuration options for the selected symbology, an Advanced button is displayed in the lower right corner of the panel. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.

Because the Hand Held Products imager does not support configuration bar codes, the Advanced function allows configuration parameters to be set for many of the supported bar codes.

Processing Order

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

Note: When Enable Code ID is set to None on the Data Options tab and when All is selected in the Symbology field, Enable and Strip Code ID on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.

When All is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

Note: In Custom mode on the Data Options tab, any Code IDs not specified by the user will not be stripped, because they will not be recognized as Code IDs.

If a specific symbology setting has been configured, a star (*) will appear next to it in the Symbology drop down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for All are used which is not necessarily the default.

Enable, Min, Max

Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the bar code data for the type of ID specified in the Data Options tab -- Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming bar code data, if the symbology is disabled, the bar code is rejected. Otherwise, the other settings in the dialog are applied and the bar code is processed.

If the symbology is disabled, all other fields on this dialog are dimmed.

If there are customized settings, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies except the customized ones.

Min

This field specifies the minimum length that the bar code data (not including Code ID) must meet to be processed.

Any bar code scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

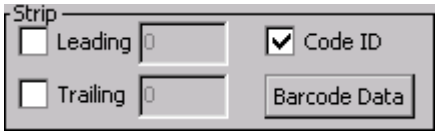
Max

This field specifies the maximum length that the bar code data (not including Code ID) can be processed. Any bar code scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

This group of controls determines what data is removed from the collected data before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.



If the total number of characters being stripped is greater than the number of characters in the collected data, it becomes a zero byte data string.

If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

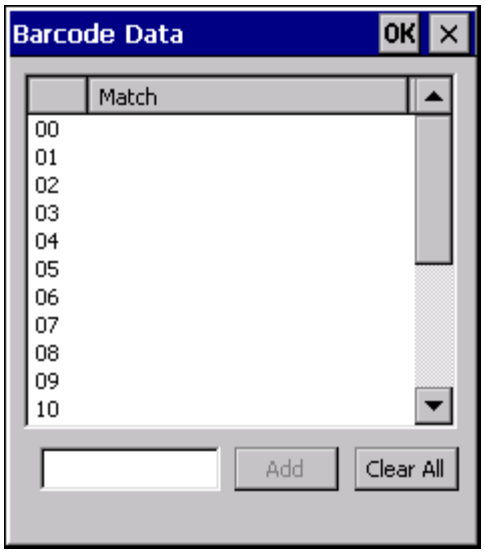
This strips the number of characters specified from the end of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Code ID

Strips the Code ID based on the type code ID specified in the Enable Code ID field in the Data Options tab. By default, Code ID stripping is enabled for every symbology (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

The Barcode Data panel is used to strip data that matches the entry in the Match list from the bar code. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.



To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap **OK** to store any additions, deletions or changes.

Barcode Data Match Edit Buttons

Add

Entering data into the text entry box enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Tap on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- Prefix and Suffix data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length bar code, a good beep will still be emitted, since bar code data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ABC and AB, in that order, incoming data with ABC will match first, and the AB will have no effect.
- When a match between the first characters of the bar code and a string from the list is found, that string is stripped from the bar code data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the bar code data. The string ABC* strips off the prefix ABC. The string *XYZ will strip off the suffix XYZ. The string ABC*XYZ will strip both prefix and suffix

together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)

- The question mark wildcard ? may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The data collected is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of Strip: Code ID in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the bar code data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the bar code data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g., <F1>), arrow keys, Page up, Page down, Home, and End.



Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the bar code data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. See Hat Encoding (page 8-38) for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix

To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string.

When bar code data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix.

The prefix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the prefix is added for any symbology that has not been specifically configured.

Add Suffix

To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string.

When bar code data is processed, the Suffix string is sent to the output buffer after the bar code data. Because all stripping operations have already occurred, stripping settings do not affect the suffix.

The suffix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the suffix is added for any symbology that has not been specifically configured.

Symbologies

The Code ID drop-down box filters the available symbologies, in the Symbology drop down box, by the selected Code ID.

When a Hand Held Products imager scan engine is installed, AIM, Custom and HHP symbologies are displayed. HHP does not support Symbol IDs.

When a Symbol scan engine is installed, AIM, Custom and Symbol symbologies are displayed. Symbol does not support HHP IDs (Hand Held Products).

AIM Symbologies

Note: When the integrated scan engine is a Symbol scan engine, AIM IDs apply, but Advanced properties do not and the Advanced button is not available.

Symbol Engine
All
Codabar
Code11
Code 39
Code 93
Code 128
Discrete 2 of 5
EAN 128
Interleaved 2 of 5
MSI
Other
PDF417
Plessey
RSS14
UPC/EAN

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

HHP Symbologies

Advanced properties are available when an integrated Hand Held Products imager is installed. Advanced properties are applicable regardless of the ID type selected (AIM or HHP). HHP = Hand Held Products.

Not all HHP symbologies have Advanced options. Click the symbology link in the table below for the symbology Advanced options.

HHP Symbology				
All	Code 128	Interleaved 2 of 5	Plessey *	UPCA *
Aztec	Composite	ISBT-1	Posi *	UPCE0 *
BPO	Coupon	Matrix 2 of 5	Postnet	UPCE1 *
Codabar *	DataMatrix	Maxicode	QR	CANPOST
CodaBlock	EAN8 *	Mesa *	RSS	AUSPOST
Code 11 *	EAN13 *	MicroPDF	Strt25	JapanPost
Code 32	EAN128	MSI	Strt32	Planet *
Code 39 *	GenCode128	OCR *	Telepen *	DutchPost
Code 49	IATA25	Other	TLC	ChinaPost
Code 93	ID Tag	PDF417	Trioptic39	Code16K
				Usps4cb

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

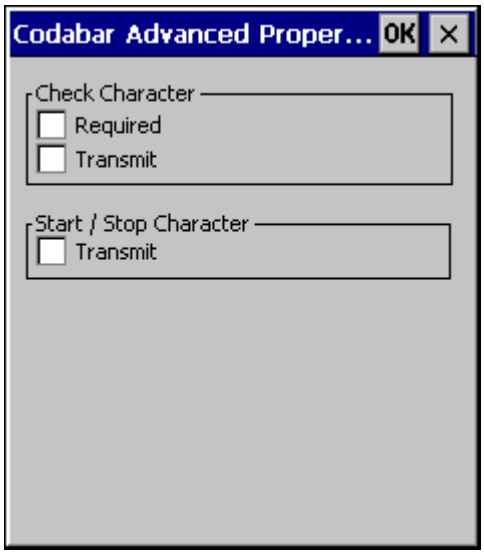
Advanced Button (Hand Held Products Imager Only)

The Advanced button is only available if a Hand Held Products Imager is in use. Because the Hand Held Products imager does not support configuration bar codes (available in the *Integrated Scanner Programming Guide*), the Advanced button function allows configuration parameters to be set for many of the HHP imager supported bar codes.

If there are advanced configuration options for the selected Hand Held Products Imager symbology, an Advanced button is displayed in the lower right corner of the panel. When the Enable check box is empty, the Advanced button is dimmed for a symbology with advanced configuration parameters. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.

Sections that follow are the HHP symbologies with advanced configuration parameters that can be changed by the user.

Codabar - Advanced Properties



Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Start / Stop Character

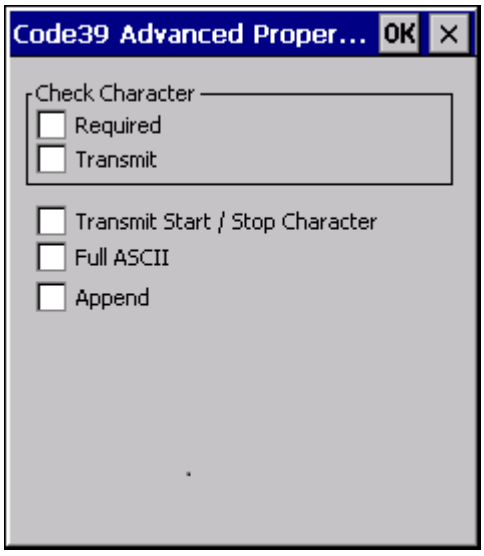
Transmit – When enabled, the start / stop characters are transmitted. Default is disabled.

Code 11 - Advanced Properties



Check Digits Required – When enabled, only bar codes with two check digits are decoded. The default is disabled.

Code 39- Advanced Properties



Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Transmit Start / Stop Character – When enabled, the start / stop characters are transmitted. Default is disabled.

Full ASCII – When enabled, full ASCII interpretation is used. Default is disabled.

Append – When enabled, append and buffer codes that start with a space. Default is disabled.

EAN 8 - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

Addenda

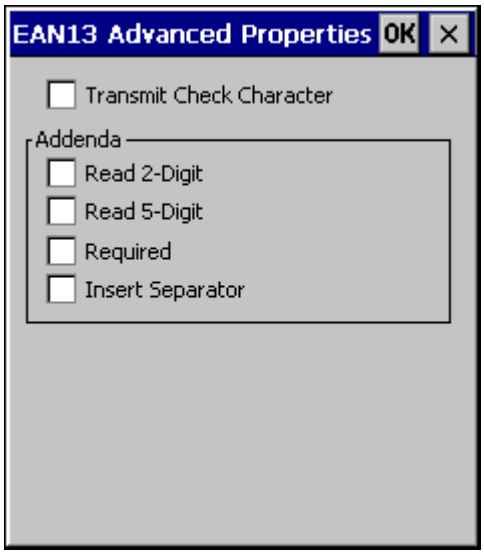
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

EAN 13 - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is disabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

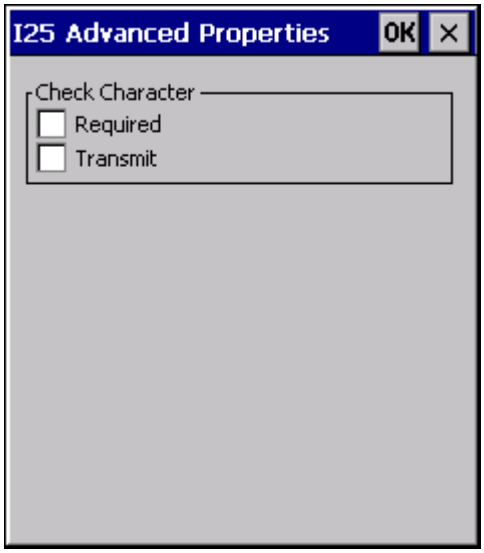
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

Note: A UPCA decoding algorithm will also decode EAN 13 labels. For correct operation, either disable the UPCA symbology when using EAN 13 labels or configure the UPCA settings to match the EAN 13 settings.

Interleaved 2 of 5 - Advanced Properties

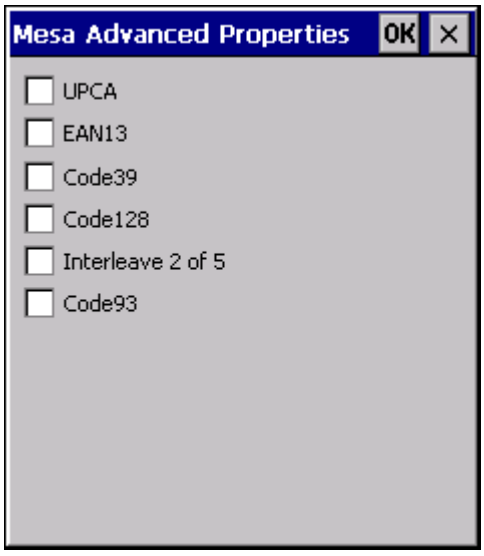


Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Mesa - Advanced Properties



UPCA – When enabled, decode UPCA Mesa. Default is disabled.

EAN13 – When enabled, decode EAN 13 Mesa. Default is disabled.

Code39 – When enabled, decode Code 39 Mesa. Default is disabled.

Code128 – When enabled, decode Code 128 Mesa. Default is disabled.

Interleaved 2 of 5 – When enabled, decode Interleaved 2 of 5 Mesa. Default is disabled.

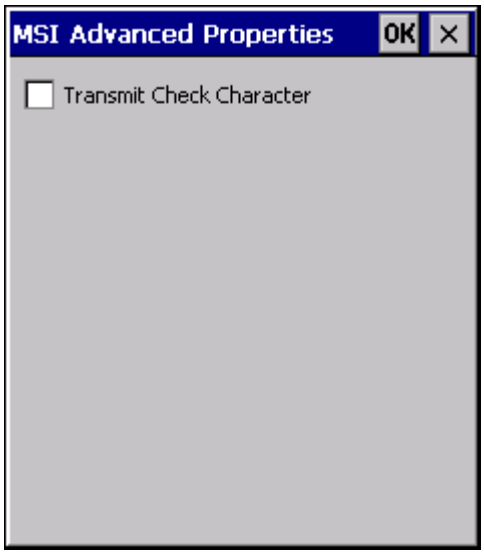
Code93 – When enabled, decode Code 93 Mesa. Default is disabled.

When the Mesa symbology is chosen on the Symbology panel (the Enable checkbox is checked) the Advanced button must be clicked and the desired Mesa Advanced Properties sub-symbology selected.

When Mesa is disabled on the Symbology panel (the Enable checkbox is cleared), click the Advanced button and uncheck all parameters or sub-symbologies, on the Mesa Advanced Properties panel.

Note: The root symbology (UPCA, EAN13, Code39, Code128, Interleaved 2 of 5 and/or Code 93) must be enabled before the matching enabled Mesa sub-symbology will decode.

MSI Plessy - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

OCR Properties - Advanced Properties



Font – Font selection. Default is disabled.

- A = OCR A
- B = OCR B
- Money = OCR Money
- MICR = Magnetic Ink Character Recognition

Direction – Decoder reads OCR fonts in any direction, but setting direction parameter correctly can increase decoding speed. Default is Left to Right.

Template – Template length must match the length of OCR string to be read. Default is dddddddd. Valid template selections are:

- a - alphanumeric character (digit or letter)
- c - check character
- d - digits from 0 to 9
- e - any character
- g - any character specified in group G
- h - any character specified in group H
- l - alphabetic letter
- r - delimits a row
- t - delimits multiple templates

All characters are transmitted as is except for the selected template.

Group G – Null terminated string defines the set of characters in group G. The default is null.

Group H – Null terminated string defines the set of characters in group H. The default is null.

Check – Enter the string constant 0123456789 for modulo10 checksums and the string constant 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ for modulo36 checksums.
The default is null.

OCR Template Examples

1. To read a combination of 6 alpha and numeric characters use the following template:

```
aaaaaa
```

2. To read the same string with a modulo 10 check digit in the seventh character position, use the following template:

   ```
   aaaaaac
   ```

   Then enter 0123456789 for the Check parameter.

3. To read either a string of 6 alphabetic letters OR a string of 8 numeric digits, use this template:

   ```
   lllllltddddddddd
   ```

   Note the use of the “t” to separate the first template from the second.

4. To read multiple rows of OCR data as shown below:

   ```
   123456
   ABCDEF
   ```

   Either of the following templates could be used:

   ```
   ddddddrllllll  or  aaaaaaraaaaaa
   ```

   Note the use of the “r” to define the position of the second row.

OCR Checksum Calculation

The following explains how the checksum is generated for the OCR bar code:

Modulo 10:

1. Add the characters in the string (not including the checksum character). Valid values are 0 – 9 for modulo 10.
2. Subtract 10 from the sum obtained above. Continue subtracting 10 until the remainder is less than 10.
3. The remainder obtained above is the checksum. Enter this digit in the checksum position.

Modulo 36:

1. Add the characters in the string (not including the checksum character). Digit / Alpha values are defined as follows for modulo 36: 0 – 9 = 0 – 9; A = 10, B = 11, … Z = 25
2. Subtract 36 from the sum obtained above. Continue subtracting 36 until the remainder is less than 36.
3. Subtract the remainder obtained above from 36. The value obtained is the checksum. Enter this character in the checksum position.

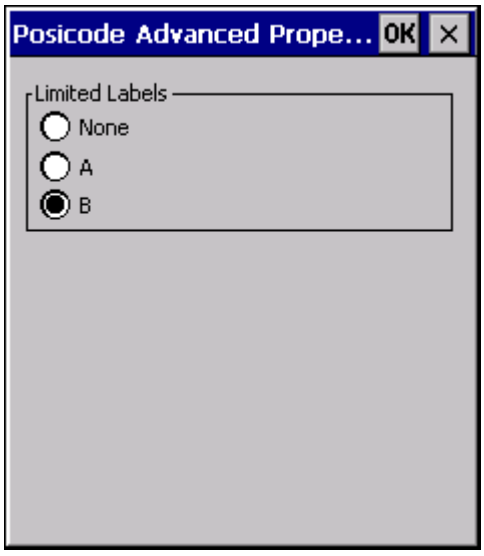
Planet - Advanced Properties

(PostaL AlphaNumeric Encoding Technique).



Transmit Check Character – When enabled, transmit the check character. Default is disabled.

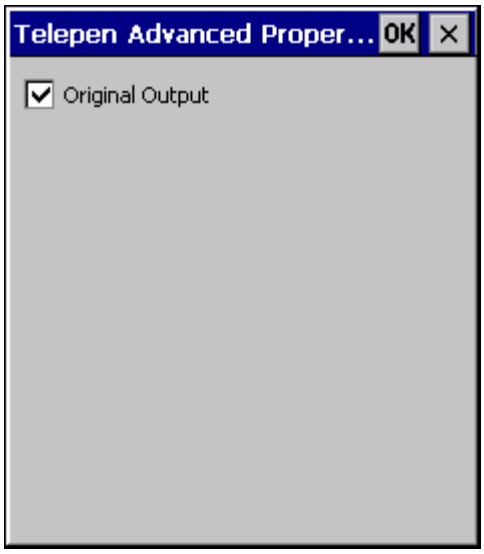
Posicode - Advanced Properties



Limited Labels – Select the type of Posicode Limited labels:

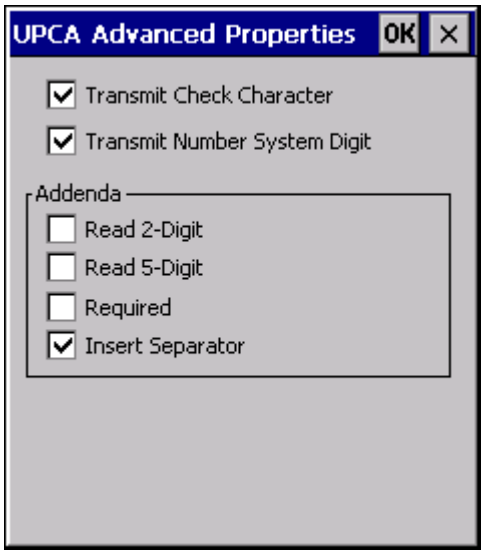
- None
- A – Posicode Limited A
- B – Posicode Limited B

Telepen - Advanced Properties



Original Output – When enabled, output is Original Telepen. When disabled, output is AIM. Default is enabled.

UPCA - Advanced Properties



Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit Number System Digit – When enabled, transmit the number system digit. Default is enabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

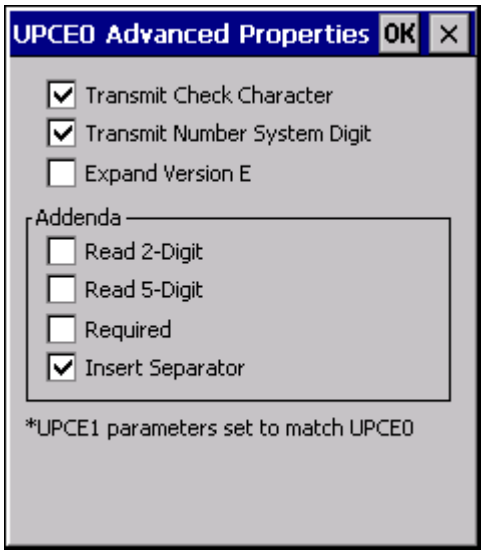
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

Note: An EAN 13 decoding algorithm will also decode UPCA labels. For correct operation, either disable the EAN 13 symbology when using UPCA labels or configure the EAN 13 settings to match the UPCA settings.

UPCE0 - Advanced Properties



Note: The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Note: UPCE0 and UPCE1 are enabled as the same symbology at the scanner. Therefore, the only way for UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it is scanned by the imager but rejected by Data Collection Wedge.

Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit number System Digit – When enabled, transmit the number system digit. Default is enabled.

Expand Version E – When enabled, expand version E to 12-digit UPCA format. Default is disabled.

Addenda

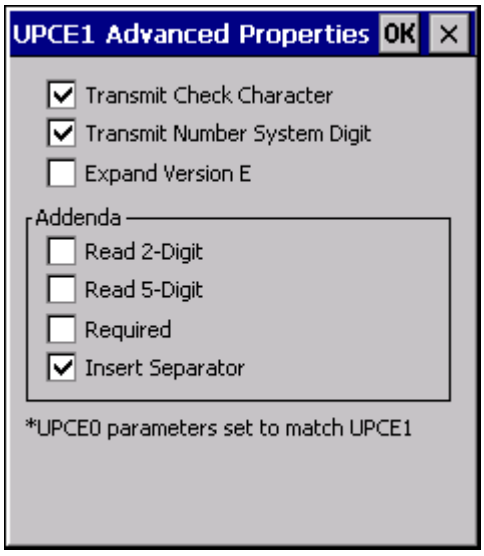
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is enabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

UPCE1 - Advanced Properties



Note: The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Note: UPCE0 and UPCE1 are enabled as the same symbology at the scanner. Therefore, the only way for UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it is scanned by the imager but rejected by Data Collection Wedge.

Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit number System Digit – When enabled, transmit the number system digit. Default is enabled.

Expand Version E – When enabled, expand version E to 12-digit UPCA format. Default is disabled.

Addenda

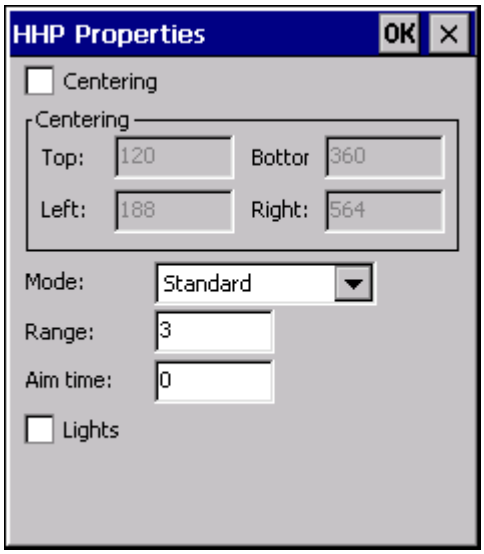
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is enabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

HHP Properties



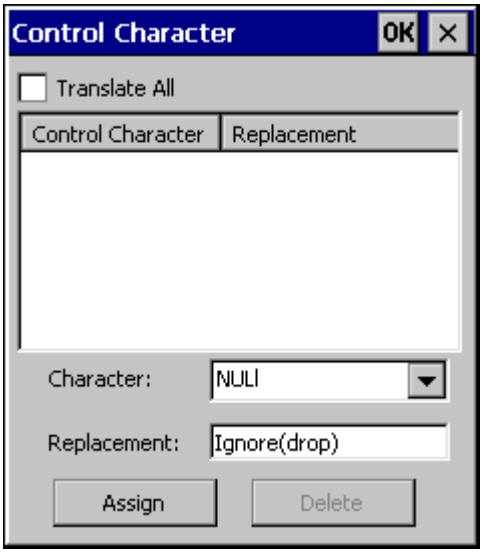
When the MX9 is equipped with a Hand Held Products imager, this option is used to configure imager parameters.

Option	Action
Centering	The centering feature is used to allow the user to accurately scan a selected bar code among a group of bar codes that are located closely together. When centering is turned on, the imager will only decode bar codes that intersect the centering window defined by the user. The centering window must intersect the center of the bar code. The default centering settings define a 60 pixel square area in the center of the imager's field of view. The default is disabled. When enabled, the following parameters may be entered. *Top* Valid:0 – 239 Default:120 *Bottom* Valid:240 – 479 Default:360 *Left* Valid:0 – 319 Default:188 *Right* Valid:320 – 639 Default:564
Mode	In Standard mode the imager will decode both linear and 2-D symbologies. In Aggressive Linear Decode mode the imager will only read linear symbologies in this mode, but decoding these is faster and more accurate than Standard Mode. In Quick Omni mode the imager searches for a bar code in a reduced field located around the center of the image. Decoding is faster in this mode, but the user must center the aiming line over the bar code to be read. Both linear and 2-D symbologies can be read in this mode. The default is Standard.
Range	Set the linear range. Valid:1 – 6 Default:3 A value of 1 specifies that the linear range that is searched for a readable label is a tight vertical range near the aimer. A value of 6 specifies that the entire height of the image is to be searched.

Option	Action
Aim Time	Duration of the imager aim beam in 0.1 second increments. Valid:0 – 50 (0 to 5 seconds) Default:0
Lights	Specifies if the imager's lights and aimer should be left on during the entire decode process. The default is disabled. If disabled, the lights are turned on only during image capture, then turned off while the imager attempts to process and decode the bar code. If enabled, the aimer and lights remain turned on during the entire process. In Aggressive Linear Decode mode, set this parameter to enabled to improve the aimer visibility. See “Mode” above.

Ctrl Char Mapping

The Ctrl Char Mapping button activates a dialog to define the operations the Data Collection Wedge performs on control characters (values less than 0x20) embedded in bar codes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.



Translate All

When Translate All is checked, unprintable ASCII characters (characters below 20H) in scanned bar codes are assigned to their appropriate CTRL code sequence when the bar codes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the bar code data, prefix, and suffix before the keystrokes are simulated.

Translate All

This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned bar code are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default Ignore (drop) in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.
For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned bar code (or defined in the prefix or suffix) will be replaced with the value 0x0a. The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.

Delete

This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Custom Identifiers

The Custom Identifiers button is located on the Data Options tab. Code IDs can be defined by the user. This allows processing parameters to be configured for bar codes that do not use the standard AIM or Symbol IDs or for bar codes that have data embedded at the beginning of the data that acts like a Code ID.

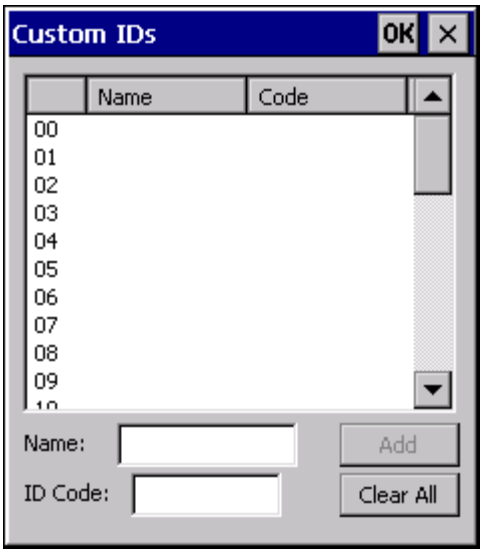
These are called “custom” Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless Enable Code ID is set to None. When the custom Code ID is found in a bar code, the configuration specified for the custom Code ID is applied to the bar code data. The dialog below allows the custom Code IDs to be configured.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if Enable Code ID is set to AIM or Symbol), or to replace the list of standard code IDs (if Enable Code ID is set to Custom).

When Enable Code ID is set to None, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

Note: When Strip: Code ID is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).



Note: After adding, changing and removing items from the Custom IDs list, tap the OK button to save changes and return to the Barcode panel.

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a bar code that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Custom ID Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Tap on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration data	**Translation**	**Example Control Character**	**Example configuration**	**Translated data**
Ignore(drop)	The control character is discarded from the bar code data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the bar code is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a bar code is converted to the text 'STX'.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	'^M'	Value 0x0d in a bar code is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	'\^I'	Value 0x09 in a bar code is converted to the text '^I'.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	'0x0A'	Value 0x0D in a bar code is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '0\x0A'	Value 0x0C is a bar code is converted to text '0x0A'

Bar Code Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	**EAN-128 (]C1)**	**EAN-13 (]E0)**	**Intrlv 2 of 5 (]IO)**	**Code93**
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Bar Code Data		‘*123’	‘1*’	‘456’	
Strip Trailing	0	0	3	3	
Prefix	‘aaa’	‘bbb’	‘ccc’	‘ddd’	
Suffix	‘www’	‘xxx’	‘yyy’	‘zzz’	

Provided that the wedge is configured with the above table, following are examples of scanned bar code data and results of these manipulations.

Bar Code Symbology	**Raw Scanner Data**	**Resulting Data**
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< rejected > (too short)
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< rejected > (too long)
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< rejected > (disabled)
Code-93	]G0444444	< rejected > (disabled)
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< rejected > (too short)

Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned bar code data by the processing causes a bad scan beep on the same data.

Length Based Bar Code Stripping

Use this procedure to create symbology rules for two bar codes with the same symbology but with different discrete lengths. This procedure is not applicable for bar codes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

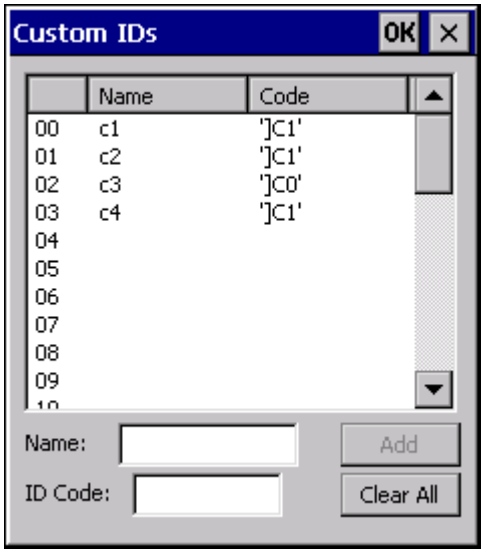
- A normal AIM or Symbol symbology role can be created for the desired bar code ID.
- Next, a custom bar code symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

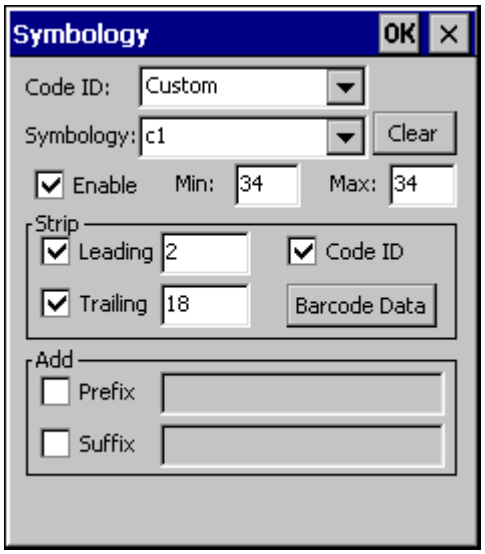
For the purposes of this example, the following sample bar code parameters will be used – EAN 128 and Code 128 bar codes. Some of the bar codes start with '00' and some start with '01'. The bar codes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character bar code is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

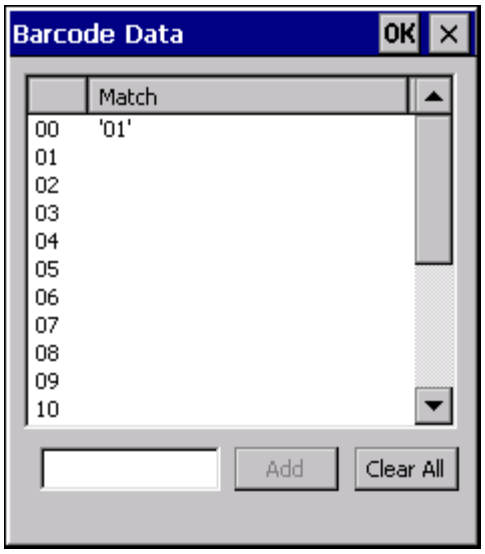
1. On the Data Options tab, set Enable Code ID to AIM.
2. Create four custom IDs, using 1 for EAN 128 bar code and 0 for Code 128 bar code.
   - c1 = Code = ']C1'
   - c2 = Code = ']C1'
   - c3 = Code = ']C0' (24 character bar code is Code 128)
   - c4 = Code = ']C1'



3. AIM custom symbology setup is assigned in the following manner:
   - c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
   - c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
   - c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
   - c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"
4. Add the AIM custom symbologies. Refer to Symbology Settings (page 8-9) for instruction.



5. Tap the Barcode Data button.
6. Tap the Add button.
7. Add the data for the match codes.



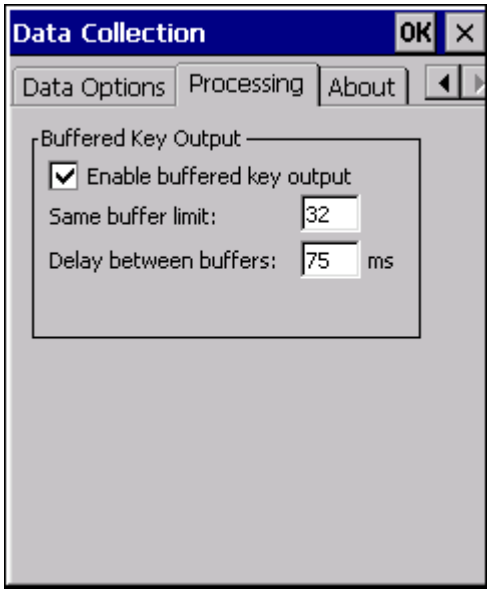
8. Refer to the previous section Barcode Data Match List (page 8-12) for instruction.
9. Scan a bar code and examine the result.

Processing Tab

The Processing tab contains a user configurable key delay that applies to scanned bar codes as they are input when Remote Desktop is the application with the input focus.

Setting	Default
Enable buffered key output	Enabled
Same buffer limit (characters)	32
Delay between (key) buffers	75 ms

Note: Settings on this panel have no effect when RFTerm is the application with the input focus.



Enable buffered key output

Default is enabled (checked). Tap the check box to turn off buffered key output.

Same buffer limit

Default is 32 ms. Raise or lower this value as desired.

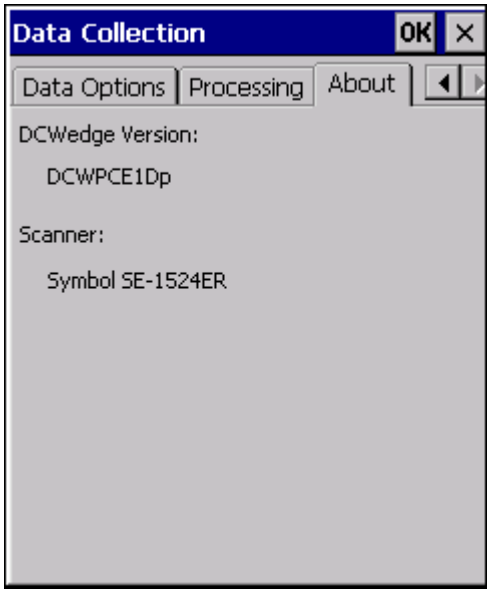
Delay between (key) buffers

Specifies the number of milliseconds to delay after each character in the scanned bar code is processed as a keystroke. This value may need to be adjusted depending on the network traffic in the environment. The default value is 75 ms. Valid value is from 0 to 9999. A zero value is No Delay between characters.

About Tab

The About tab lists the version of the Data Collection Wedge (DCWedge) software and the type of scanner/imager installed in the MX9.





Valid scanner / imager types:

- HHP – Hand Held Products 5300 2D Imager
- Symbol – Symbol SE955
- Symbol – Symbol SE1524
- No Scanner/None – No scanner installed

Hat Encoding

Hat Encoded Characters Hex 00 through AD.

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Hat Encoded Characters Hex AE through FF.

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

9 Enabler Installation and Configuration

Introduction

This section discusses Honeywell supported features with Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the follow additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler

Supported devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the \System folder.

Note: Important: If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.

The Avalanche Enabler installation file HSM_ENABLER_CAB is loaded on the MX9 by Honeywell; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

After installation the Enabler will run as a background application monitoring for updates. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

The RMU.CE.CAB file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the RMU (Remote Management Utility) after the MX9 reboots.

Enabler Uninstall Process

To remove the Avalanche Enabler from the MX9:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the MX9.

The Avalanche folder cannot be deleted while the Enabler is running. See Stop the Enabler Service (page 9-2).

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the MX9, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the MX9 desktop.
2. Select **File > Settings**.
3. Select the **Preferences** tab.
4. Select **Do not monitor** to prevent automatic monitoring upon Startup.
5. Select **Exit Application** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Click the **OK** button to save the changes.
7. Reboot the MX9 if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the MX9 can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the MX9.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the MX9.
- Wirelessly via the MX9 2.4GHz radio and an access point

After installing the Enabler on the MX9 the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the MX9 will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using bar code wedge panels on the MX9).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the MX9 must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. See Enabler Configuration (page 9-4) for details.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the MX9 Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE devices

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the desktop.
2. Select **File > Settings**.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for **Manage Network Settings**, **Manage Wireless Settings** and **Use Avalanche Network Profile**.
6. Click the **OK** button to save the changes.
7. Reboot the device.

Preparing a Device for Remote Management

Two additional utilities are necessary for remote management.

Remote Management Utility (RMU)

The Remote Management Utility (RMU) must be installed on all mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties.

If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed.

Important: If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB).

If the amount of storage RAM is too low, the Enabler returns a “Mobile unit out of resources” error.

To determine the minimum value required, inspect the RMU.StorageSpaceAvailable>=nn parameter in the Criteria field for the OS package. Generally, this setting should be approximately the amount of storage space available on the Storage Card.

For example, if after installing all the software, the device shows 5MB in use, this setting should be about 45MB for a standard OS, 55 MB for an Asian font OS.

Wireless Configuration Application (WCA)

Use the Wireless Configuration Application (WCA) when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

User Interface

The Enabler can be configured and controlled manually through the user interface on the MX9. This section details the functionality that can be controlled by the user or system administrator.

Screen displays shown in this section are designed to present the end-user with information graphically.

Placement of information on the screen displays may be split between one or many tabbed panels.

Standard Avalanche Enabler parameters that are not supported by Honeywell may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

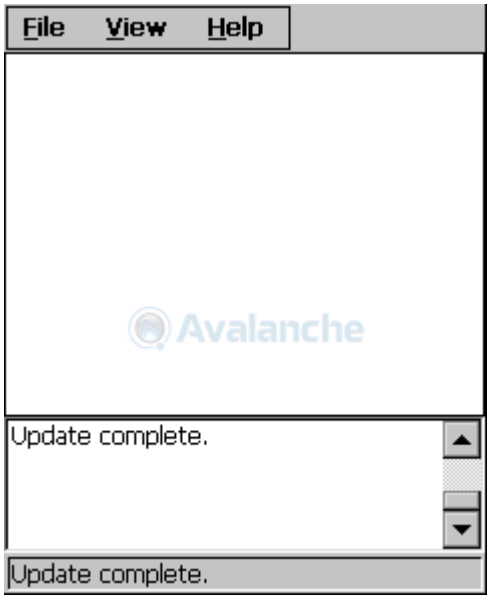
Enabler Configuration

Depending on the version of the Enabler running on the MX9, the Enabler icon may look like one of the following:

 or  Enabler Settings Icon

The Enabler user interface application is launched by clicking either the Enabler Settings icon on the desktop or Taskbar or by selecting Avalanche Enabler from the Programs menu.

The opening screen presents the MX9 user with the connection status and a navigation menu.



Note: Some parameters and features described in this section may not be available until you are running the latest version of the Enabler.

File Menu Options

Connect

The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the MX9 immediately upon a successful connection.

Scan Config

Scan Configuration feature not supported. The Scan Config option under the File menu allows the user to configure Enabler settings using a special bar code that can be created using the Avalanche MC Console utilities. Refer to the Wavelink Avalanche Mobility Center User Guide for details.

Settings

The Settings option under the File menu allows the MX9 user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected.



The default Settings password is **system**. The password is not case-sensitive.

Avalanche Update using File > Settings

Use these menu options to setup the Avalanche Enabler on the MX9. Change the settings and then save the changes (reboot) before connecting to the network.

Alternatively, the Mobile Device Server can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details).

Menu Options

Note: Your MX9 screen display may not be exactly as shown in the following menu options. Contact Technical Assistance (page 15-1) for version information and upgrade availability.

Connection

Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.

Execution

Not available in this release. Use AppLock (page 6-1) instead, which is resident on each Windows device.

Server Contact

Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.

Data

Control when data is transferred between the device and the Mobile Device Server.

Preferences

Set options for Enabler startup or shutdown and logging. Replaces Startup/Shutdown tab in some Enabler versions.

Taskbar

Set options for Taskbar.

Scan Config

This option allows the user to configure Enabler settings using a special bar code that is created by the Avalanche Mobility Center console. *Scan Config not currently supported.*

Display

Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.

Shortcuts

Add, delete and update shortcuts to user-allowable applications.

SaaS

Configure the Enabler to connect with Avalanche on Demand.

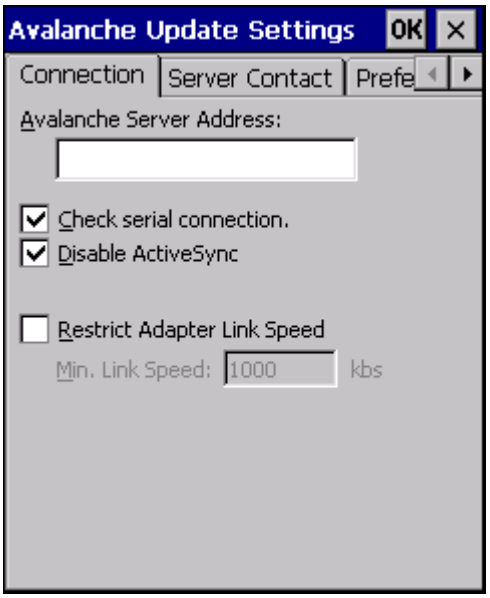
Adapters

Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.

Status

View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection



Avalanche Server Address

Enter the IP Address or host name of the Mobile Device Server assigned to the MX9.

Check Serial Connection

Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.

Disable ActiveSync

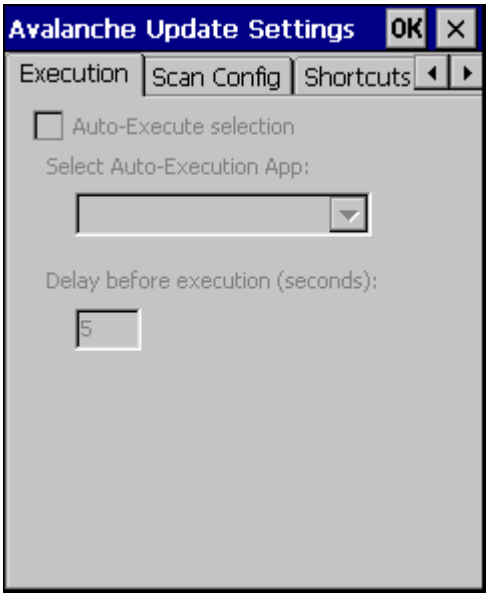
Disable ActiveSync connection with the Mobile Device Server.

Restrict Adapter Link Speed

Default is disabled. Minimum Link Speed dimmed.

Execution

Note the dimmed options on this MX9 panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.



Auto-Execute Selection

An application that has been installed with the Avalanche Management system can be run automatically following each boot.

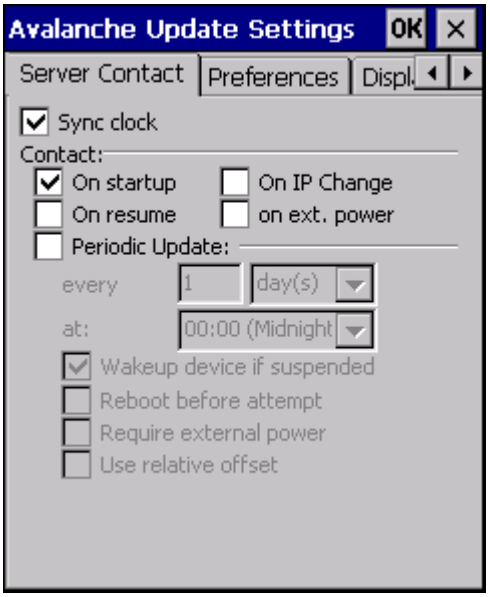
Select Auto-Execute App

The drop-down box provides a list of applications that have been installed with the Avalanche Management System.

Delay before execution

Time delay before launching Auto-Execute application.

Server Contact



Note: Your MX9 screen display may not be exactly as shown above. Contact Technical Assistance (page 15-1) for upgrade availability and version information.

Sync Clock

Reset the time on the MX9 based on the time on the Mobile Device Server host PC.

Contact

On Startup – Connect to the Mobile Device Server when the Enabler is accessed.

On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.

On IP Change - Connect to the Mobile Device Server when the IP address of the MX9 changes.

On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.

Periodic Update

Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.

Wakeup device if suspended

If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.

Reboot before attempt

Reboot mobile device before attempting to contact Mobile Device Server.

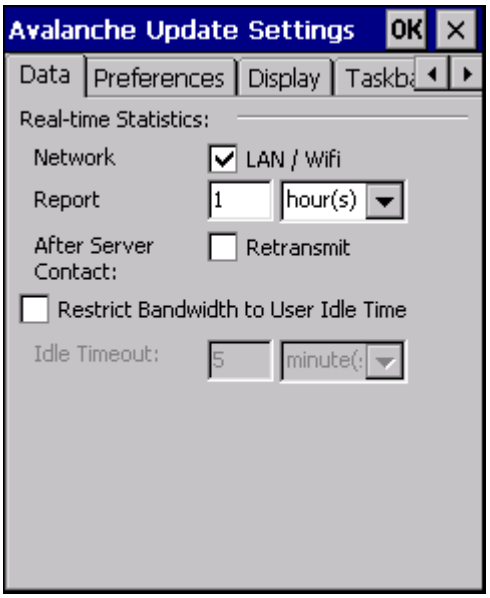
Require external power

Only connect when the mobile device has external power.

Use relative offset

Dimmed.

Data



The Data tab controls when data is transferred between the MX9 and the Mobile Device Server.

Transfer Data When Device is Idle

When enabled, periodic updates from the Mobile Device Server are postponed until the MX9 has been idle for the specified period of time. The default is disabled.

Idle timeout

Specify the length of time the device must be idle before a periodic update can run, used when the parameter above is enabled.

Real-time Statistics

When checked, the statistics are transmitted over the network by the Enabler.

Report

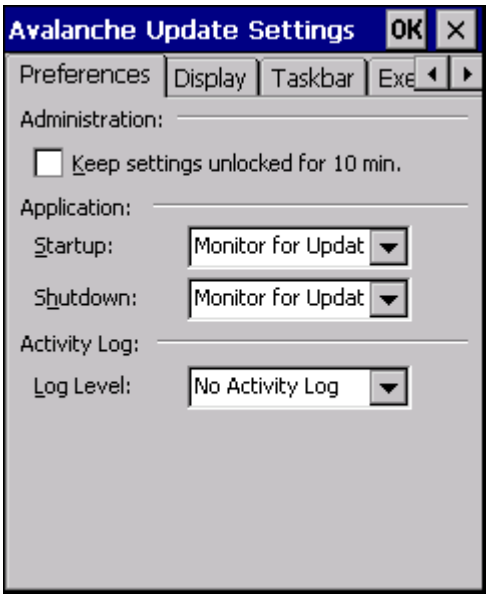
Specifies the Report Interval, how frequently the Enabler reports statistics to the Mobile Device Server.

Retransmit After Server Contact

Specifies if the device sends statistics to the Mobile Device Server immediately following a connection to the server.

Preferences

For best results, use AppLock (page 6-1) to manage the taskbar. AppLock is resident on each mobile device.



Administration

By default, *Keep settings unlocked for 10 minutes* is disabled (checkbox is blank).

Application

Startup

Behavior of the Enabler when the MX9 boots up. The default is Monitor for Updates.

- Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
- Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
- Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.

Shutdown

Behavior of the monitor when the Enabler is exited. The default is Monitor for Updates.

- Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
- Exit Application - Terminates the monitor (requires successful password entry if a password has been configured).

Activity Log

Log Level

Use this option to control the level of detail recorded in the log file. The default is No Activity Log.

- No Activity Log - No log file is written.
- Critical - Only critical errors written to the log files.
- Error - Communication or configuration problems are written to the log file along with critical messages.
- Warning - Possible operation problems are written to the log file along with critical and error messages.
- Info - Operational information is written to the log file.
- Debug - The most detailed log file.

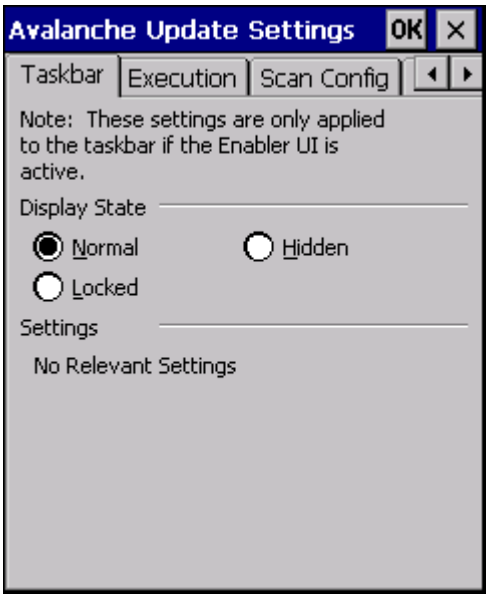
Display Level

Use this option to control the level of detail shown on the main Enabler screen. The default is Basic Output.

- Basic Output - General information is displayed.
- Critical - Critical errors are displayed in addition to those above.
- Error - Communication or configuration problems are displayed in addition to those above.
- Warning - Possible operation problems are displayed in addition to those above.
- Info - Operational information is displayed in addition to those above.
- Debug - The most detailed list is displayed.

Taskbar

For best results use AppLock (page 6-1) to manage the taskbar. AppLock is resident on each mobile device.

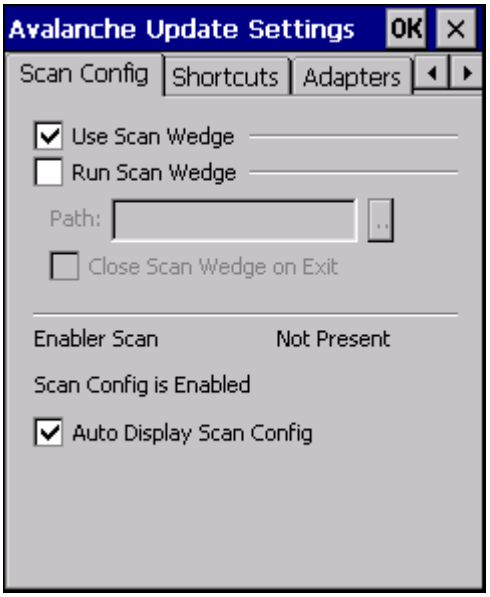


The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed.
- Locked - taskbar is visible, but most icons are hidden or for information only.

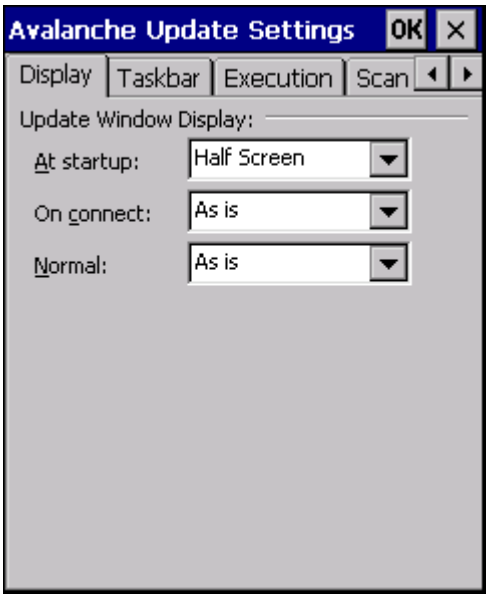
Scan Config

For best results use eXpress Config and eXpress Scan for this function. eXpress Scan is included with the updated MX9 enablers.



Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is not currently supported on the MX9.

Display



The user interface for the Enabler can be configured to dynamically change based on the status of the MX9 connection with the Mobile Device Server.

At startup

Default is Half Screen. Options are Half screen, Hidden or Full screen.

On connect

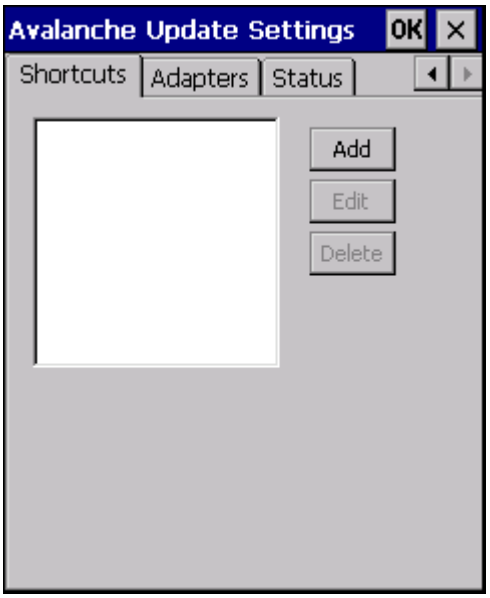
Default is As Is. Options are As is, Half screen, or Full screen.

Normal

Default is As Is. Options are Half screen, Hidden or As Is.

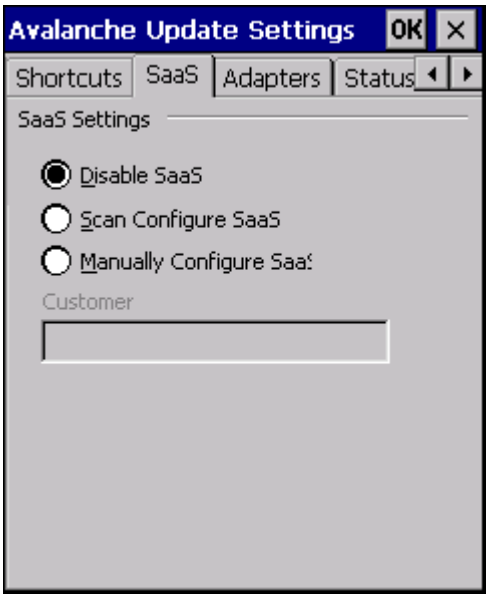
Shortcuts

For best results use AppLock (page 6-1) for this function. AppLock is resident on each mobile device.



Configure shortcuts to other applications on the MX9. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

SaaS



Use to configure the Enabler to connect with Avalanche on Demand. This is a Software-as-a-Service version of Avalanche. Using either of the SaaS configuration options below assumes the user has registered with Wavelink.

Disable SaaS

No SaaS connection is used.

Scan Configure SaaS

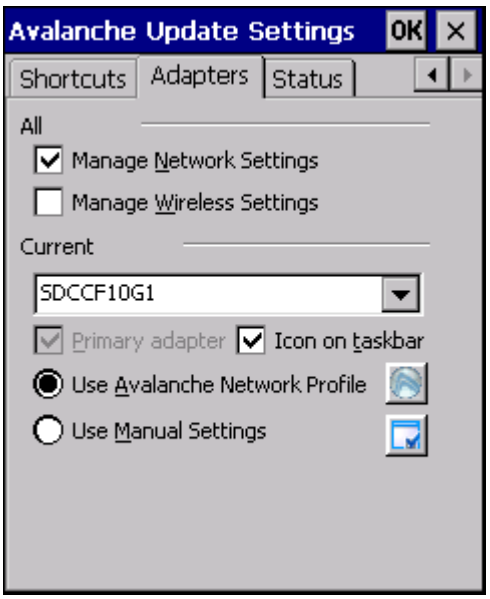
Scan bar codes printed from within the Avalanche Console to configure the Enabler for the SaaS connection.

Manually Configure SaaS

Manually enter the SaaS connection information. Enter the server address on the Connection tab and the customer ID in the Company text box.

Adapters

Note: Review the network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet.



Manage Network Settings

When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.

Manage Wireless Settings

When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked as configuration packages provide more radio configuration options.

Current Adapter

Lists all network adapters currently installed on the MX9.

Primary Adapter

Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).

Icon on taskbar

Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.

Use Avalanche Network Profile

The Enabler will apply all network settings sent to it by the Mobile Device Server.

Avalanche Icon

Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.

Use Manual Settings

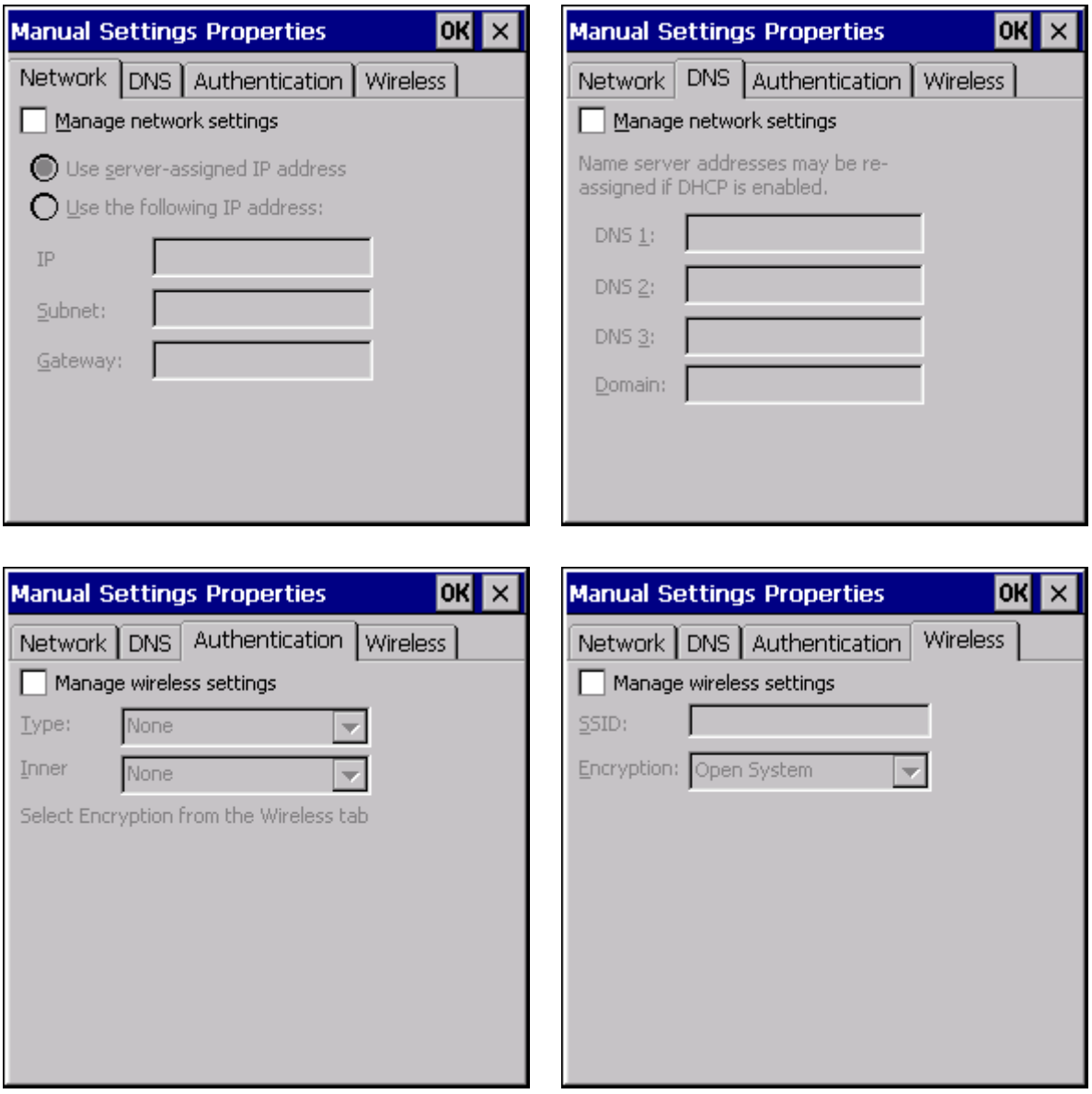
When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the MX9.

Properties Icon

Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.

Manual Settings Properties)



Note: The Authentication tab may not be present in all versions of the Enabler.

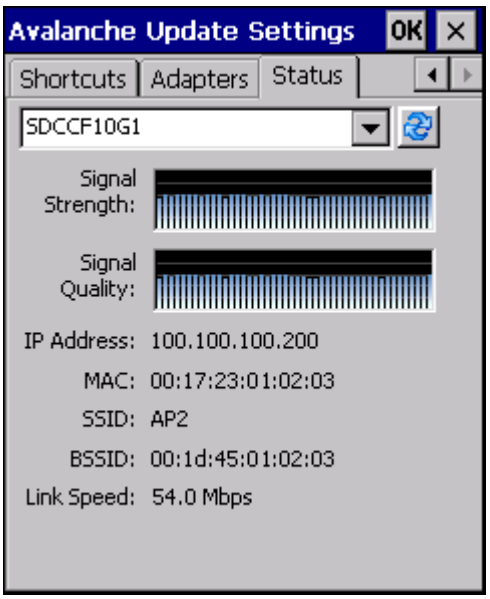
Do not enable *Manage Wireless Settings* for Summit Client devices.

Note: When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel. Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the MX9 network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



Link speed indicates the speed at which the signal is being sent from the adapter to the MX9. Speed is dependent on signal strength.

Exit

The Exit option is password protected. The default password is leave. The password is not case-sensitive.



If changes were made on the MX9 Startup/Shutdown tab screen, then after entering the password, tap **OK** and the following screen is displayed:



Change the option if desired. Tap the X button to cancel Exit. Tap the **OK** button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the MX9 is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double click the MX9 enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the MX9.

Using eXpress Scan



eXpress Scan Desktop Icon

If the MX9 has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device.

If the eXpress Scan icon is not present on the desktop, install the Enabler. If the icon is still not present, the Enabler must be updated.

If the eXpress Scan icon is present, follow these steps to configure the MX9 to connect with the wireless network and the Mobile Device Server.

Creating Bar Codes

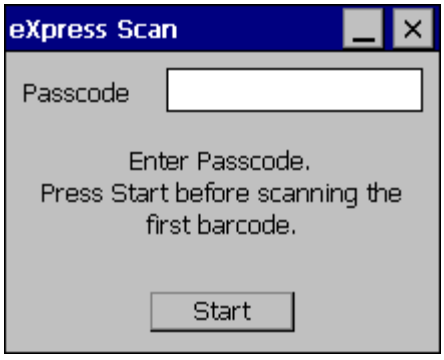
Barcodes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the bar code length and the number of parameters selected, eXpress Config generates one or more bar codes for device configuration. The bar codes contain configuration parameters for the wireless client in the mobile device and may also specify the address of the Mobile Device Server.

Barcodes should be printed at a minimum of 600 dpi.

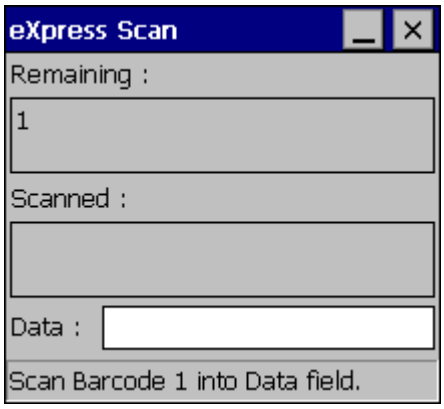
Scanning Bar Codes

Follow these instructions for each device to be configured.

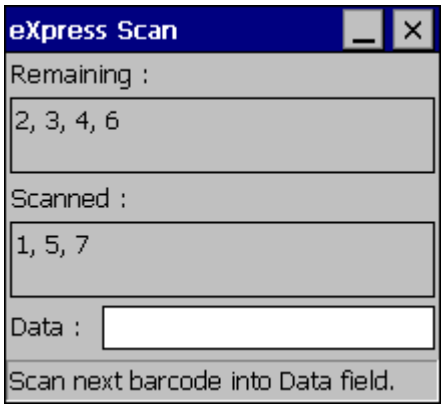
1. Start eXpress Scan on the MX9 by double clicking the eXpress Scan icon.
2. Enter the bar code password, if any.



3. Click Start.
4. Bar code 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the bar codes were created.



5. If the passwords match, the bar code data is processed and the screen is updated to reflect the number of bar codes included in the set.
6. If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Bar code 1 scanned again.



7. The remaining bar codes may be scanned in any order. After a bar code is scanned, that bar code is removed from the "Remaining:" list and placed in the "Scanned:" list.

Process Complete

After the last bar code is scanned, the settings are automatically applied.



Once configured, the MX9 is warmbooted. Once connected to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

10 Wireless Network Configuration

Introduction

The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates or an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Security options supported are:

- No Security (page 10-21)
- WEP (page 10-22)
- LEAP (page 10-23)
- PEAP/MSCHAP (page 10-24)
- PEAP/GTC (page 10-26)
- WPA/LEAP (page 10-28)
- EAP-FAST (page 10-29)
- EAP-TLS (page 10-31)
- WPA PSK (page 10-33)

Important Notes

⚠	It is important that all dates are correct on the MX9 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
⚠	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance (page 15-1) for details.
⚠	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, perform a Warmboot.

Summit Client Utility

Note: When making changes to profile or global parameters, tap the power key to place the MX9 in Suspend. When the MX9 resumes from suspend the parameters are applied. The MX9 can be resumed by tapping the power key or the touch screen or by pressing any key.

Select the Summit Client Utility using the Start button or tap the Summit Tray Icon (if present).

The Main Tab (page 10-3) provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile Tab (page 10-6). The parameters on this tab can be set to unique values for each profile.

The Status Tab (page 10-10) contains information on the current connection.

The Diags Tab (page 10-11) provides utilities to troubleshoot the radio.

Global parameters are found on the Global Tab (page 10-12). The values for these parameters apply to all profiles.

Help

Help is available by clicking the ? icon in the title bar on most Summit Client Utility (SCU) screens. Help may also be accessed by selecting **Start > Help** and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

 The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Tap the icon to launch the SCU. Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. Use the Summit Client Utility to connect to your network. The Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

Using the Wireless Zero Config Utility

1. Select **ThirdPartyConfig** in the Active Profile drop down list as the active profile. See Main Tab (page 10-3).
2. Open the Registry (page 5-56) panel and tap Warmboot.

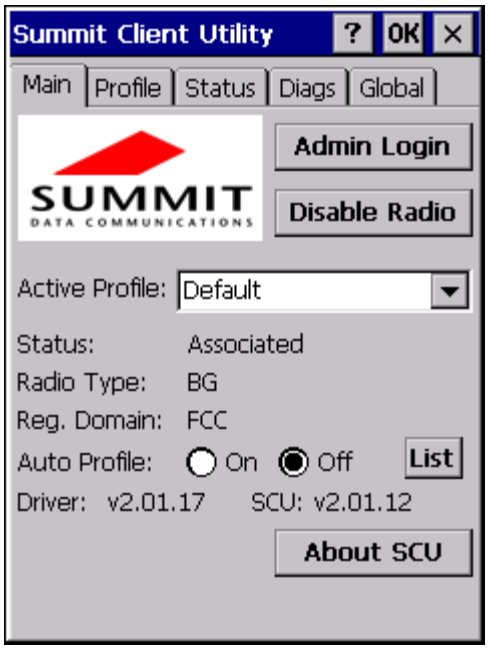
The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

Switching Control to SCU

1. To switch back to SCU control, select any other profile in the SCU Active Config drop down list, except ThirdPartyConfig.
2. Open the Registry (page 5-56) panel and tap Warmboot. Radio control is passed to the SCU.

Main Tab

Setting	Default
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	Varies by location



The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version.
- Driver version.
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11 a/b/g radio).

- Regulatory Domain is preset to either Worldwide or a location specific domain (FCC, ETSI, KCC or TELEC).
- Copyright Information can be accessed by tapping the About SCU button.
- Active Config profile / Active Profile name.
- Status of the client (Down, Associated, Authenticated, etc).

The Active Profile can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Always perform a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Wireless Manager for configuration of all client and security settings for the network module.

The Disable Radio button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

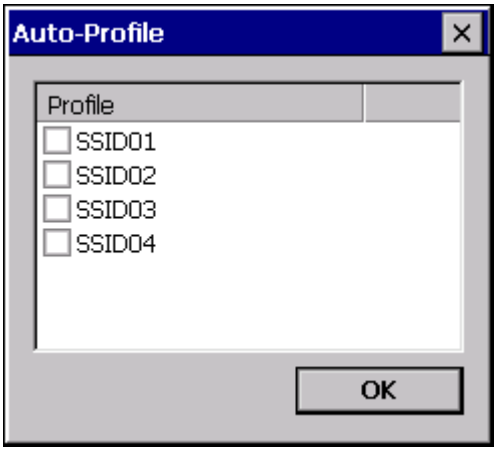
The Admin Login button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, tap the List button.



The Auto Profile selection screen displays all currently configured profiles. Tap on the check box for any profiles that are to be included in Auto Profile selection then tap **OK** to save.

To enable Auto Profile, tap the On button on the Main tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is tapped to turn off Auto Profile.

Note: Do not include any profiles with an Ad Hoc Radio Mode in this listing.

Admin Login

To login to Administrator mode, tap the Admin Login button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the Admin Logout button, or the OK button to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.



Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Main Tab (page 10-3).

The end-user can:

- Turn the radio on or off on the Main Tab (page 10-3).
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile Tab (page 10-6).
- View the global parameter settings on the Global Tab (page 10-12).
- View the current connection details on the Status Tab (page 10-10).
- View radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags Tab (page 10-11).

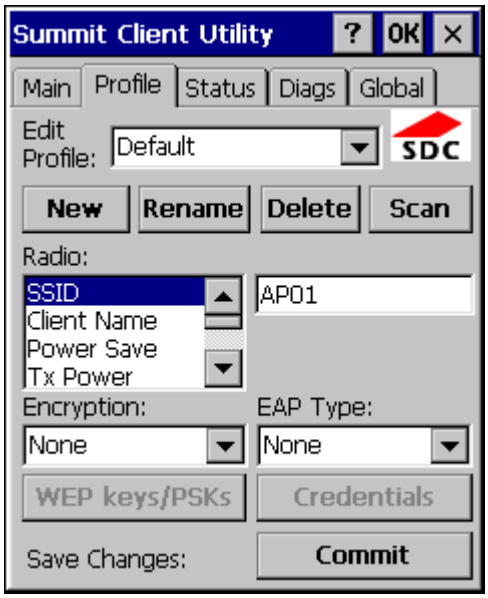
After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile tab.
- Edit global parameters on the Global tab.
- Enable/disable the Summit tray icon in the taskbar.

Profile Tab

*Note: Tap the **Commit** button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the **Commit** button, changes are not saved!*

Setting	Default
Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters for default
Auth Type	Open
EAP Type	None
Encryption	None



When logged in as an Admin use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Note: The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Buttons

New Button

Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.

Rename Button

Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.

Delete Button

Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.

WEP Keys / PSK Keys Button

Allows entry of WEP keys or pass phrase as required by the type of encryption.

Credentials Button

Allows entry of a user name and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.

Commit Button

Saves the profile settings made on this screen. Settings are saved in the profile.

Scan Button

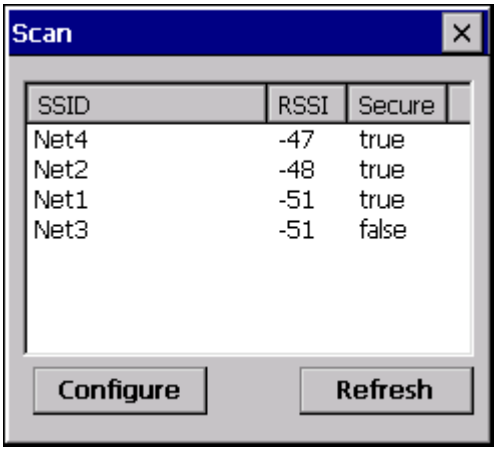
Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs.

Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false).

Sort the list by tapping on the column headers.

If you are logged in as an Admin, tap an SSID in the list then tap the Configure button. You return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name already exists).

If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security..



*Note: Unsaved Changes – The SCU will display a reminder if the **Commit** button is not tapped before an attempt is made to close or browse away from this tab.*

Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g., Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, or EAP-TLS. *Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.*
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the MX9. *Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.*

Parameter	Default	Explanation
Radio Mode	BG radio: BG Rates Full Or A radio: BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio installed in the mobile device. Options: • B rates only (1, 2, 5.5 and 11 Mbps) • BG Rates Full (All B and G rates) • G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) • BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) • A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) • ABG Rates Full (All A rates and all B and G rates with A rates preferred) • BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) • Ad Hoc (when connecting to another client device instead of an AP Default: • BG Rates Full (for 802.11b/g radios) • BGA Rates Full (for 802.11a/b/g radio) *Note: BG radio only - Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.*

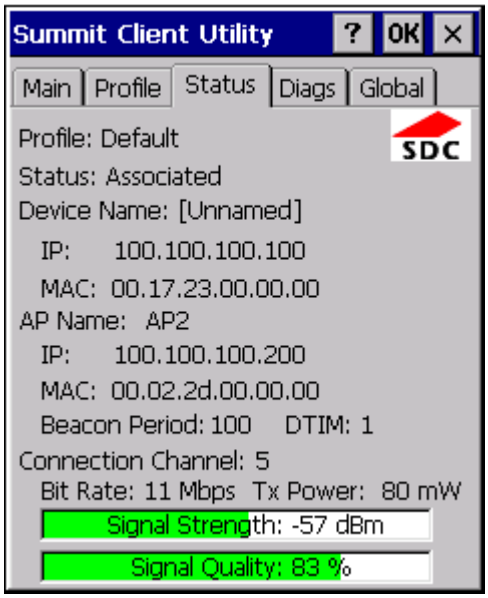
It is important the Radio Mode parameter correspond to the Access Point (AP) to which the device is to connect. For example, if this parameter is set to G rates only, the MX9 may only connect to APs set for G rates and not those set for B and G rates.

The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	Radio Mode
A Main and BG Main	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Contact Technical Assistance (page 15-1) if you have questions about the antenna(s) installed on your MX9.

Status Tab



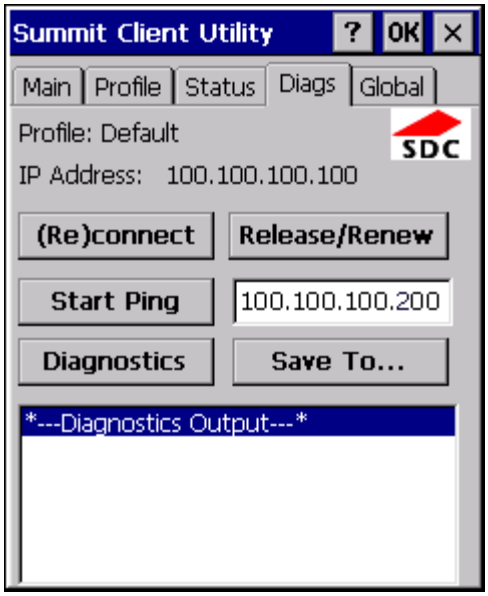
This screen provides information on the radio:

- The profile being used.
- The status of the radio card (down, associated, authenticated, etc.).
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic.
- Bit rate in Mbit.
- Current transmit power in mW
- Beacon period – the time between AP beacons in kilomicroseconds. (one kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically.
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

(Re)connect Button

Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.

Release/Renew Button

Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.

Start Ping Button

Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is tapped, the ping begins and the button label changes to Stop Ping. Clicking the button ends the ping. The ping also ends when any other button on this screen is tapped or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.

Diagnostics Button

Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.

Save To… Button

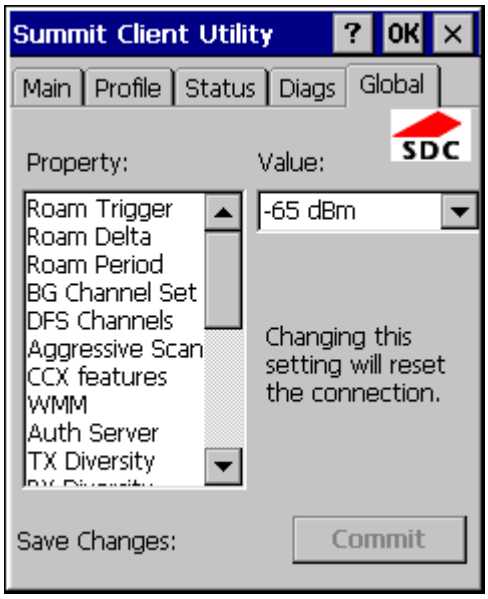
Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

The parameters on this panel can only be changed when an Admin is loggin in. The current values for the parameters can be viewed by the general user without requiring a password.

*Note: Tap the **Commit** button to save changes. If the panel is closed before tapping the **Commit** button, changes are not saved!*

Setting	**Default**
Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full
DFS Channels	Off
Ad Hoc Channel	1
Aggressive Scan	On
CCX	BG: Off A: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	BG: On A: Main Only
RX Diversity	BG: On-Start on Main A: Main Only
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms



Custom Parameter Option

Honeywell does not support the property Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Global Parameters

Parameter	Default	Function
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	BG: 10 sec. A: 5 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: • Full (all channels) • 1,6,11 (the most commonly used channels) • 1,7,13 (for ETSI and TELEC radios only) • Custom
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. *Note: Not supported (always off) in some SCU releases.*

Parameter	Default	Function
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: • 1 through 14 (the 2.4GHz channels) • 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX or CCX Features	BG: Off A: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as “On” in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP, CHAP, EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The re-authentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The re-authentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK *Note: This change does not take effect until after a Suspend/Resume cycle.*
WAPI	Off	Default is Off and dimmed (cannot be changed).

Parameter	Default	Function
TX Diversity	BG: On A: Main Only	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas). TX Diversity option should be set based on the antenna configuration as follows: • Antenna Configuration: A Main and BG Main. TX Diversity: Main. • Antenna Configuration: A Main and A Aux. TX Diversity: On. • Antenna Configuration: BG Main and BG Aux. TX Diversity: On.
RX Diversity	BG: On-Start on Main A: Main Only	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna). RX Diversity option should be set based on the antenna configuration as follows: • Antenna Configuration: A Main and BG Main. RX Diversity: Main. • Antenna Configuration: A Main and A Aux. RX Diversity: On-start on Main. • Antenna Configuration: BG Main and BG Aux. RX Diversity: On-start on Main.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.

Parameter	Default	Function
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certifcates store. The Windows folder must exist before assigning the path in this parameter. See Windows Certificate Store vs. Certs Path (page 10-19) for instructions on obtaining CA and User Certificates. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
Ping Payload	32 Bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password, the Summit Client Utility offers these choices:

- The User name and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The User name and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the User name and Password at that time to authenticate.

Using Stored Credentials

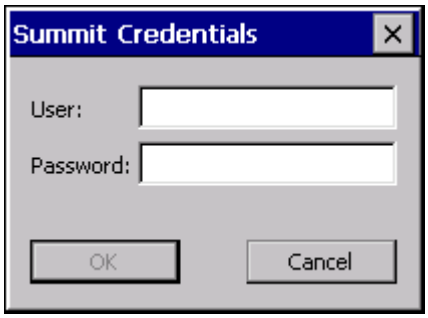
1. After completing the other entries in the profile, tap on the Credentials button.
2. Enter the User name and Password on the Credentials screen and tap the OK button.
3. Tap the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the Validate server and Use MS store check boxes are enabled.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Tap the **OK** button then the **Commit** button.
12. If changes are made to the stored credentials, tap **Commit** to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: See Configuring Profiles (page 10-21) for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

Using a Sign On Screen

1. After completing the other entries in the profile, tap on the Credentials button. Leave the User name and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the Validate server and Use MS store check boxes are enabled.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
7. Tap the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the User name and Password. Tap the OK button.



10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status Tab (page 10-10) indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot.

Note: See Configuring Profiles (page 10-21) for more details.

If a user enters invalid credentials and taps OK, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user taps the **Cancel** button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the Reconnect button on the Diags Tab is tapped or
- the profile is modified and the **Commit** button is tapped.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the MX9 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate (page 10-38).
- To import the user certificate into the Windows certificate store, see Installing a User Certificate (page 10-44).
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates:

- Imported into the Windows certificate store.
- Copied into the Certs Path directory.

Using the Certs Path

1. See Generating a Root CA Certificate (page 10-34) and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not enable the Use MS store check box after enabling the Validate server check box.
4. Enter the certificate name in the CA Cert text box.
5. Tap **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Using the Windows Certificate Store

1. See Generating a Root CA Certificate (page 10-34) and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See Installing a Root CA Certificate (page 10-37).
3. When completing the Credentials screen for the desired authentication, be sure to enable the *Use MS store* check box after enabling the *Validate server* check box.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate tap on the **Browse (…)** button.



6. Tap to uncheck (and disable) the Use full trusted store check box.
7. Select the desired certificate and tap the Select button to return the selected certificate to the CA Cert text box.
8. Tap **OK** to exit the Credentials screen and then tap **Commit** to save the profile changes.

Configuring Profiles

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. See your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

1. On the Main Tab, tap the Admin Login button and enter the password.
2. Edit the default profile with the parameters for your network. Select the Default profile from the pull down menu.
3. Make any desired parameter changes as described in the applicable following section determined by network security type and tap the **Commit** button to save the changes.

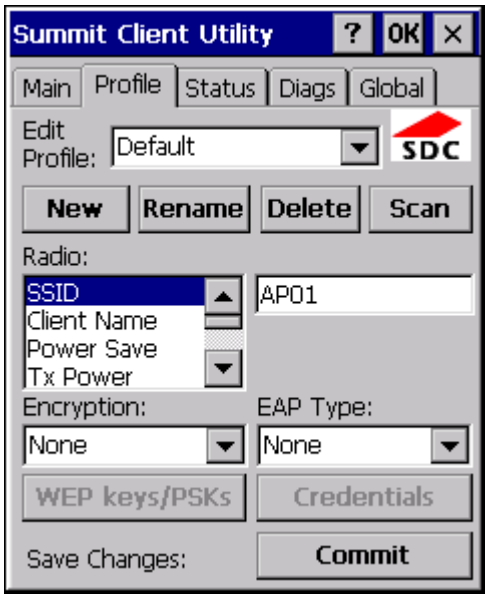
IMPORTANT – Remember to tap the **Commit** button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the **Commit** button is not tapped before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the stored credentials, tap **Commit** to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to None.
4. Set Auth Type to Open.

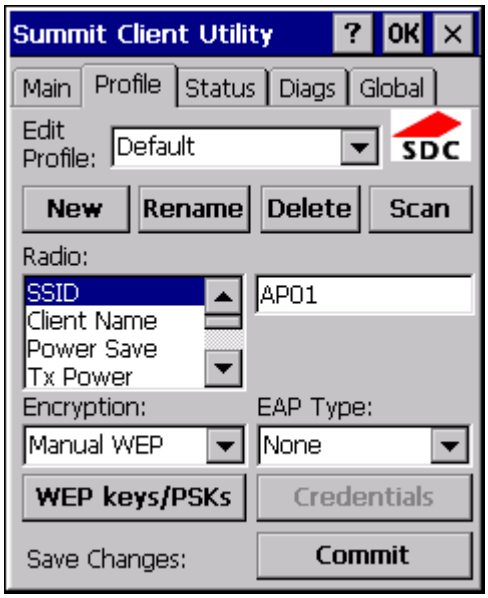


5. Once configured, tap the **Commit** button.
6. Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

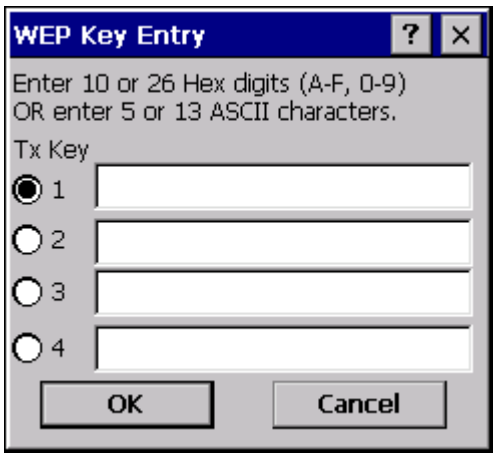
WEP

To connect using WEP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to WEP or Manual WEP (depending on SCU version).
4. Set Auth Type to Open.



5. Tap the WEP keys/PSKs button.



6. Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and tap **OK**.
7. Once configured, tap the **Commit** button.
8. Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

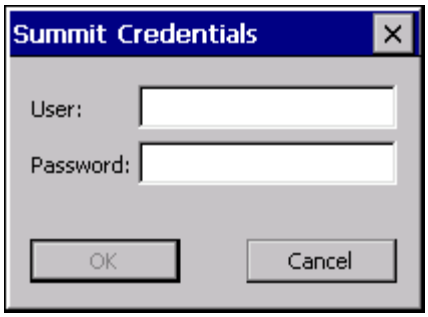
LEAP

To use LEAP (without WPA), make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to LEAP.
3. Set Encryption to WEP EAP or Auto WEP (depending on SCU version).
4. Set Auth Type as follows:
   - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
   - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to Shared.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.



5. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials.
6. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



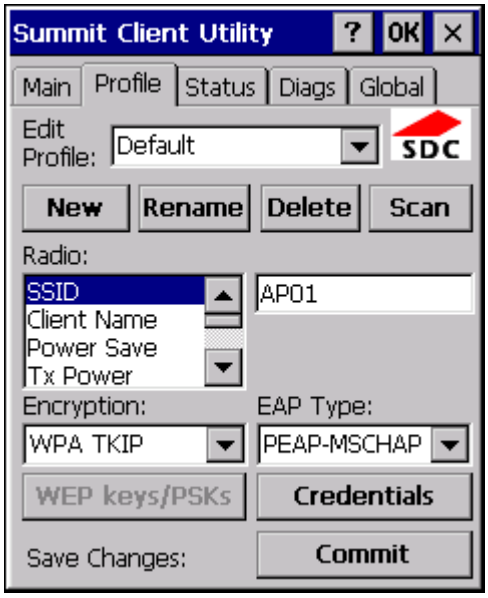
7. Enter the Domain\User name (if the Domain is required), otherwise enter the User name.
8. Enter the password. Tap **OK** then tap the **Commit** button.
9. Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

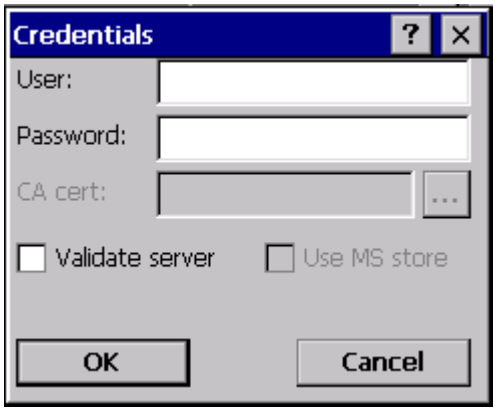
Note: The date must be properly set on the device to authenticate a certificate.

To use PEAP/MSCHAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-MSCHAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

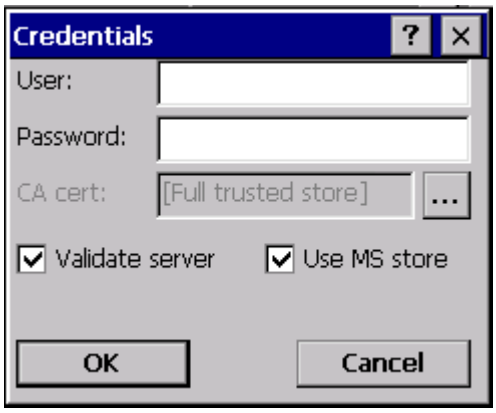


6. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials.
7. Tap the Credentials button.
   - No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
   - For Stored Credentials, User, Password and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\User name (if the Domain is required), otherwise enter the User name.

10. Enter the password.
11. Leave the CA Certificate File Name blank for now.
12. Tap **OK** then tap **Commit**. Ensure the correct Active profile is selected on the Main Tab.
13. See Windows Certificate Store vs. Certs Path (page 10-19) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.
15. Return to the Credentials screen and enable the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.

Tap **OK** then tap **Commit**.

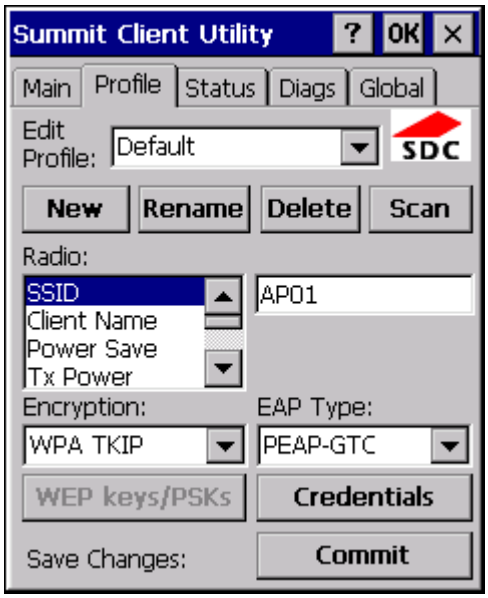
The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

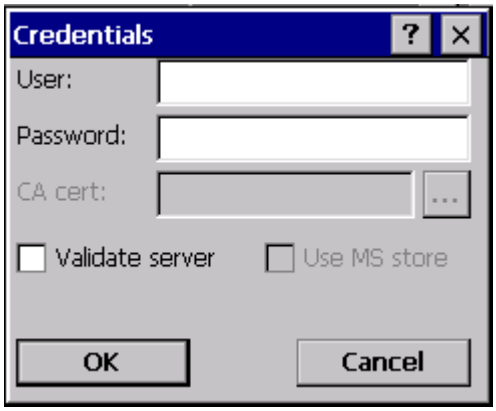
PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-GTC.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials.
7. Tap the Credentials button. No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
8. Enter these items as directed below.



9. Enter the Domain\User name (if the Domain is required), otherwise enter the User name.
10. Enter the password.
11. Leave the CA Certificate File Name blank for now.
12. Tap **OK** then tap **Commit**. Ensure the correct Active Profile is selected on the Main Tab.

13. See Windows Certificate Store vs. Certs Path (page 10-19) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.
15. Return to the Credentials screen and enable the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Tap **OK** then tap **Commit**.

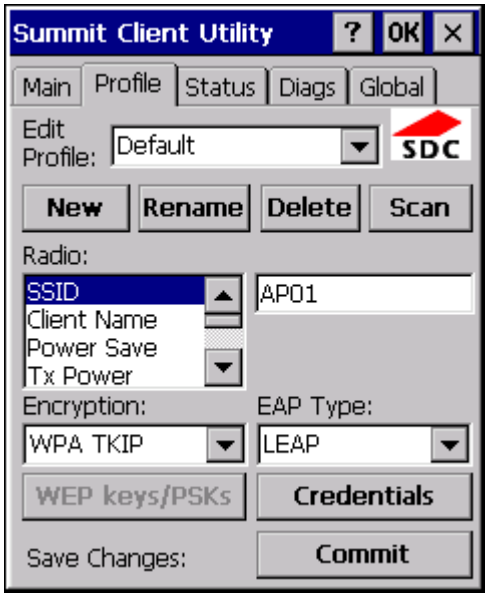
The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

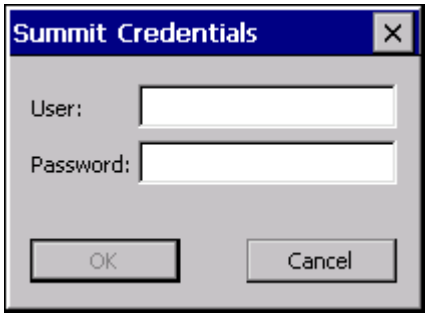
WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to LEAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type as follows:
   - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
   - If the AP is configured to used shared key or passphrase, set the Auth Type radio parameter to Shared.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials.
7. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



8. Enter the Domain\User name (if the Domain is required), otherwise enter the User name.
9. Enter the password.
10. Tap **OK** then tap the **Commit** button.
11. Ensure the correct Active Profile is selected on the Main Tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-FAST

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the MX9.

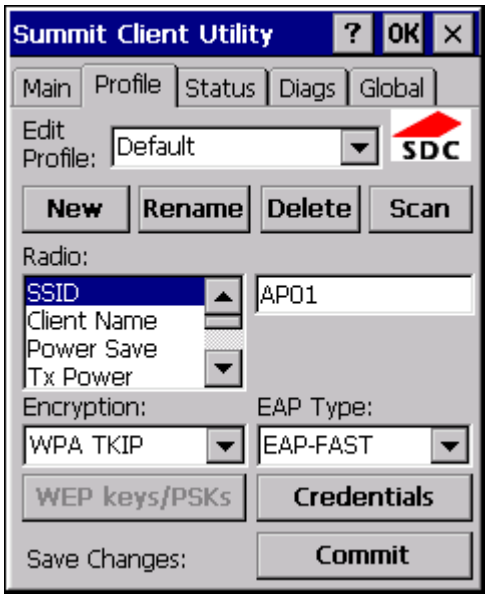
For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the MX9. The same username/password must be used to authenticate each time. See the note below for more details.

Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System folder with the PAC credentials. if the username is changed, that file must be deleted. the filename is autoP.00.pac.

For manual PAC provisioning, the PAC filename and Password must be entered.

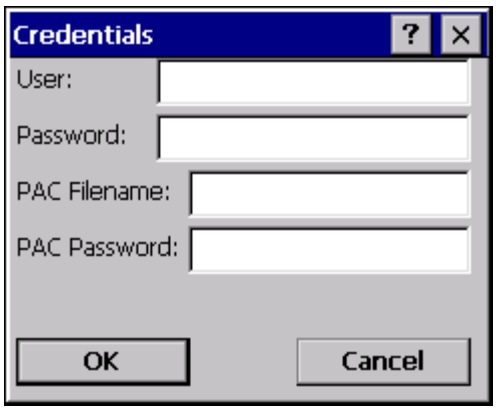
To use EAP-FAST, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-FAST.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials. The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).
7. Tap on the Credentials button.

8. To use Stored Credentials, tap on the Credentials button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the User name and Password when connecting to the network.

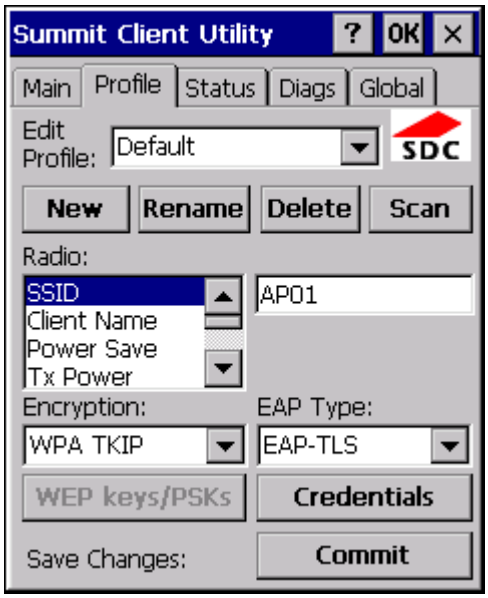


9. To use Sign-On credentials:
   - Do not enter a User and Password as the user will be prompted for the User name and Password when connecting to the network.
10. To use Stored Credentials:
    - Enter the Domain\User name (if the Domain is required), otherwise enter the User name.
    - Enter the password.
11. To use Automatic PAC Provisioning no additional entries are required.
12. To use manual PAC Provisioning:
    - Enter the PAC Filename and PAC Password.
    - The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.
13. Tap **OK** then tap the **Commit** button.
14. Ensure the correct Active Profile is selected on the Main Tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

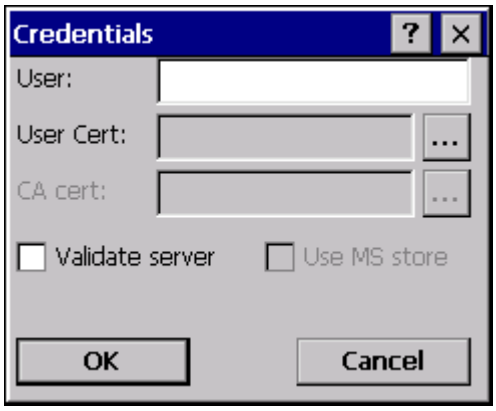
EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-TLS.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 10-17) for information on entering credentials.
7. Tap the Credentials button.
   - No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name when connecting to the network.
   - For Stored Credentials, User and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\User name (if the Domain is required), otherwise enter the User name.

10. Select a user certificate from the Windows certificate store. Use the Browse button to locate the User Cert from the certificate store. Highlight the desired certificate and press the Select button. The name of the certificate is displayed in the User Cert box.
11. Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.
12. If there are no user certificates in the Windows certificate store, generate and install a user certificate.
13. See Windows Certificate Store vs. Certs Path (page 10-19) for more information on CA certificate storage.
14. Tap the Validate server check box.



If using the Windows certificate store:

1. Tap the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, tap on the Browse button.
3. Tap to uncheck the Use full trusted store check box.
4. Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.

Tap **OK** then tap **Commit**.

The MX9 should be authenticating the server certificate and using EAP-TLS for the user authentication.

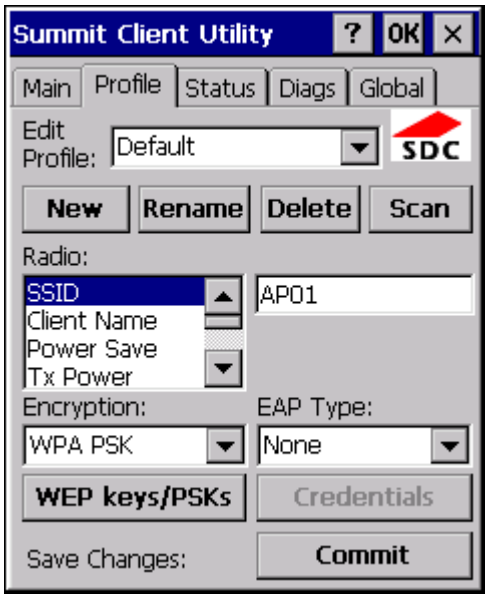
Ensure the correct Active Profile is selected on the Main tab and Wamboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Generate a Root CA certificate or a User certificate.

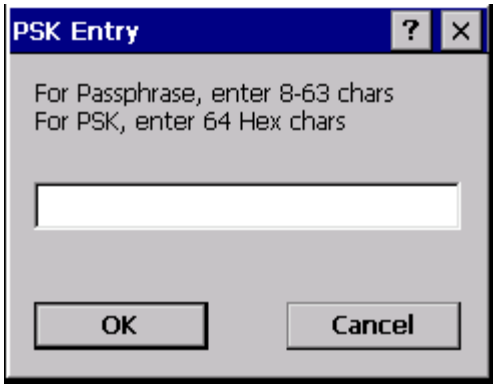
WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to WPA PSK or WPA2 PSK.
4. Set Auth Type to Open.



5. Tap the WEP keys/PSKs button.



6. This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and tap **OK**.
7. Once configured, tap the **Commit** button.
8. Ensure the correct Active Profile is selected on the Main tab and Warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Refer to the Security Primer (available at www.honeywellaidc.com) to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the MX9 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. See Generating a Root CA Certificate (page 10-34) and download the Root CA Certificate to a PC.
2. Connect the MX9 to the desktop PC using ActiveSync and copy the certificate to the MX9 \System folder.
3. See Installing a Root CA Certificate (page 10-37) and install the Root CA Certificate.

User Certificates are necessary for EAP-TLS.

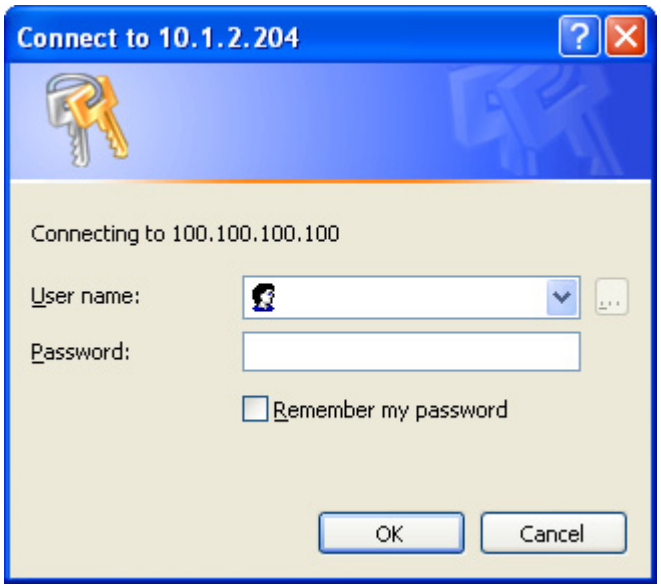
1. See Generating a User Certificate (page 10-38) and download the User Certificate and Private Key file to a PC.
2. Connect the MX9 to the desktop PC using ActiveSync and copy the certificate and private key file to the MX9 \System folder.
3. See Installing a User Certificate (page 10-44) and install the User Certificate and Private Key file.
4. After installation, perform a Warmboot.
5. Verify Installation (page 10-47).

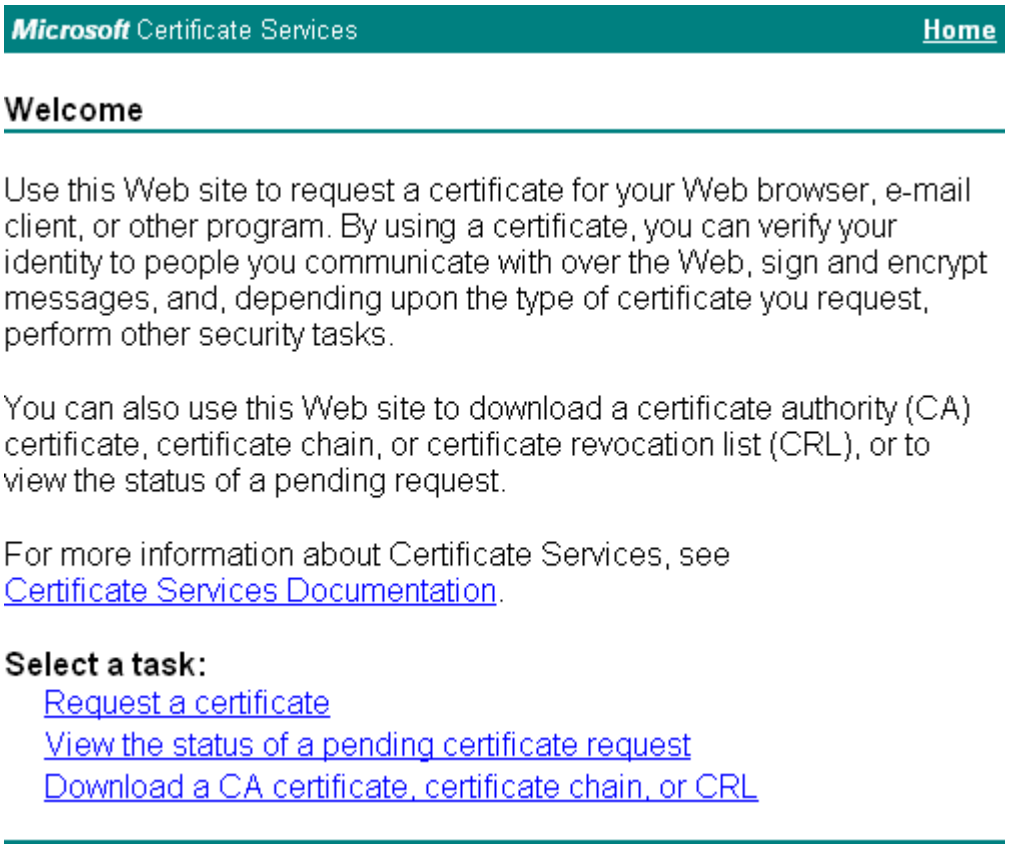
Generating a Root CA Certificate

Note: It is important that all dates are correct on the MX9 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

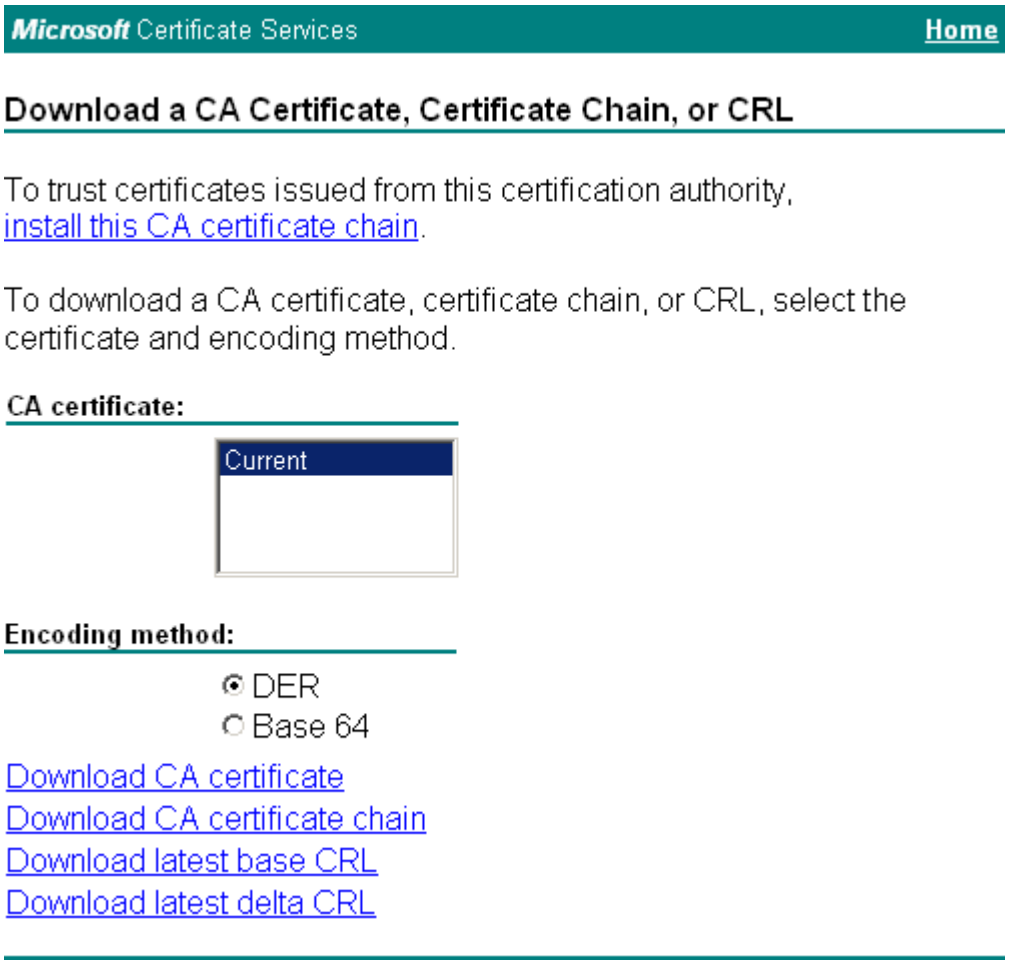
The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority.

1. To request the root CA certificate, open a browser to http://<CA IP address>/certsrv.
2. Sign into the CA with any valid username and password.

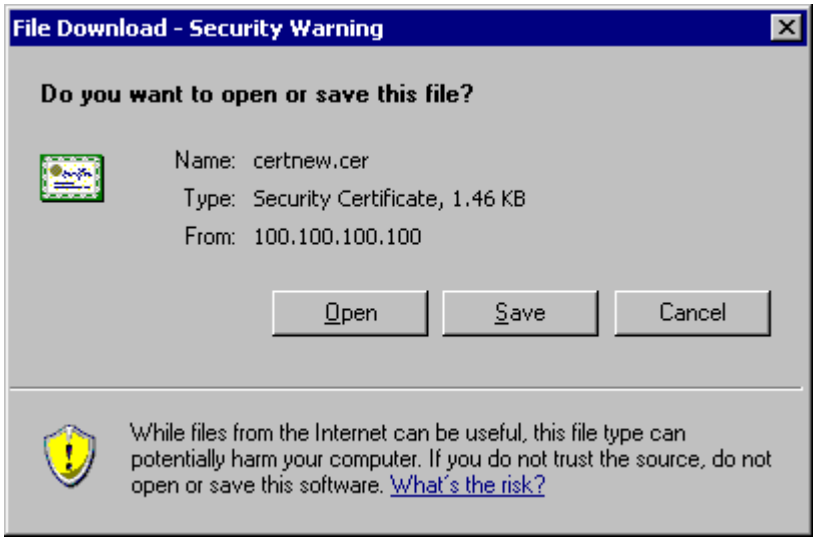



Microsoft Certificate Services
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Click the Download a CA certificate, certificate chain or CRL link.
4. Make sure the correct root CA certificate is selected in the list box.


Microsoft Certificate Services
Home
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, install this CA certificate chain.
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:
Current
Encoding method:
DER
Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

5. Click the DER button.
6. To download the CA certificate, click on the Download CA certificate link.


File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.46 KB
From: 100.100.100.100
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

7. Click the Save button and save the certificate. Make sure to keep track of the name and location of the certificate.

8. Install the certificate on the MX9.

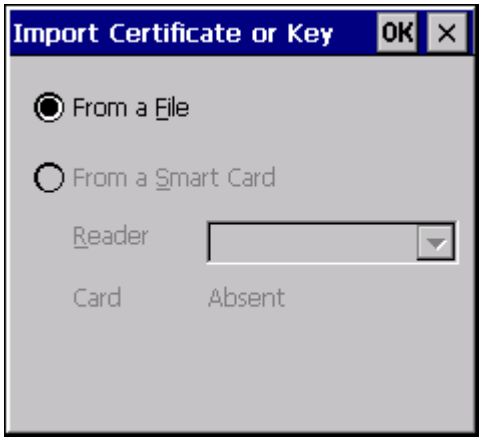
Installing a Root CA Certificate

Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

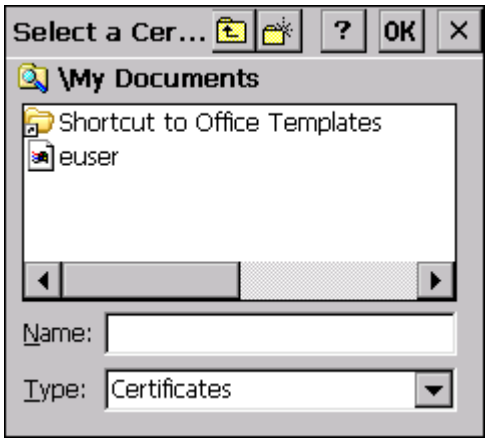
Copy the certificate file to the MX9. Import the certificate by navigating to **Start > Control Panel > Certificates.**



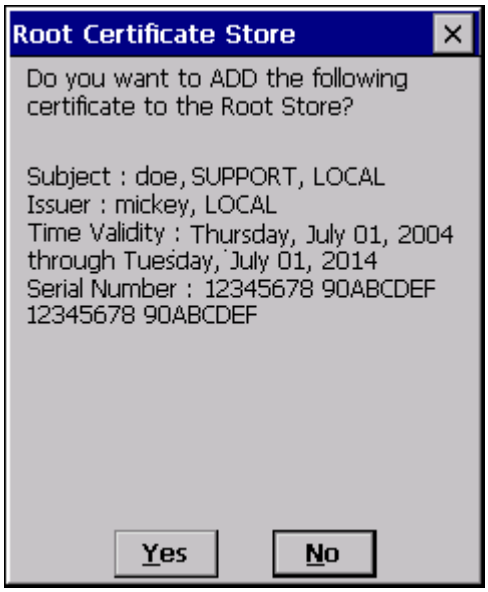
9. Tap the Import button.



10. Make sure From a File is selected and tap **OK**.



11. Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

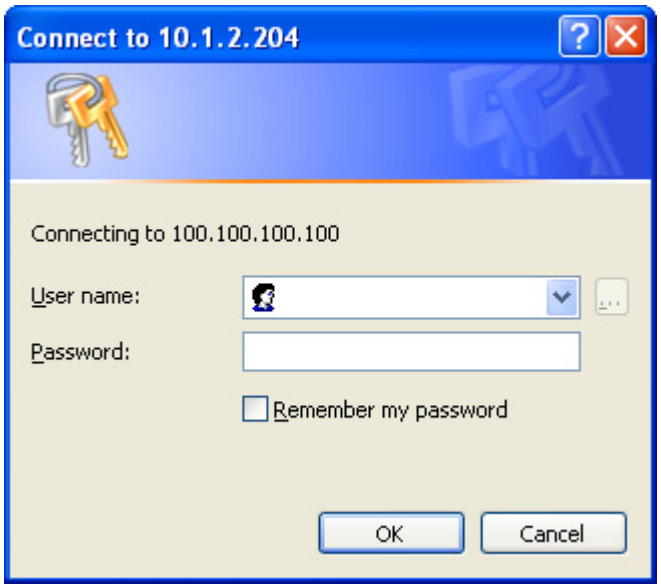

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : doe, SUPPORT, LOCAL
Issuer : mickey, LOCAL
Time Validity : Thursday, July 01, 2004 through Tuesday, July 01, 2014
Serial Number : 12345678 90ABCDEF 12345678 90ABCDEF
Yes
No

12. Tap Yes to import the certificate.
13. Once the certificate is installed, return to the proper authentication section, earlier in this manual.

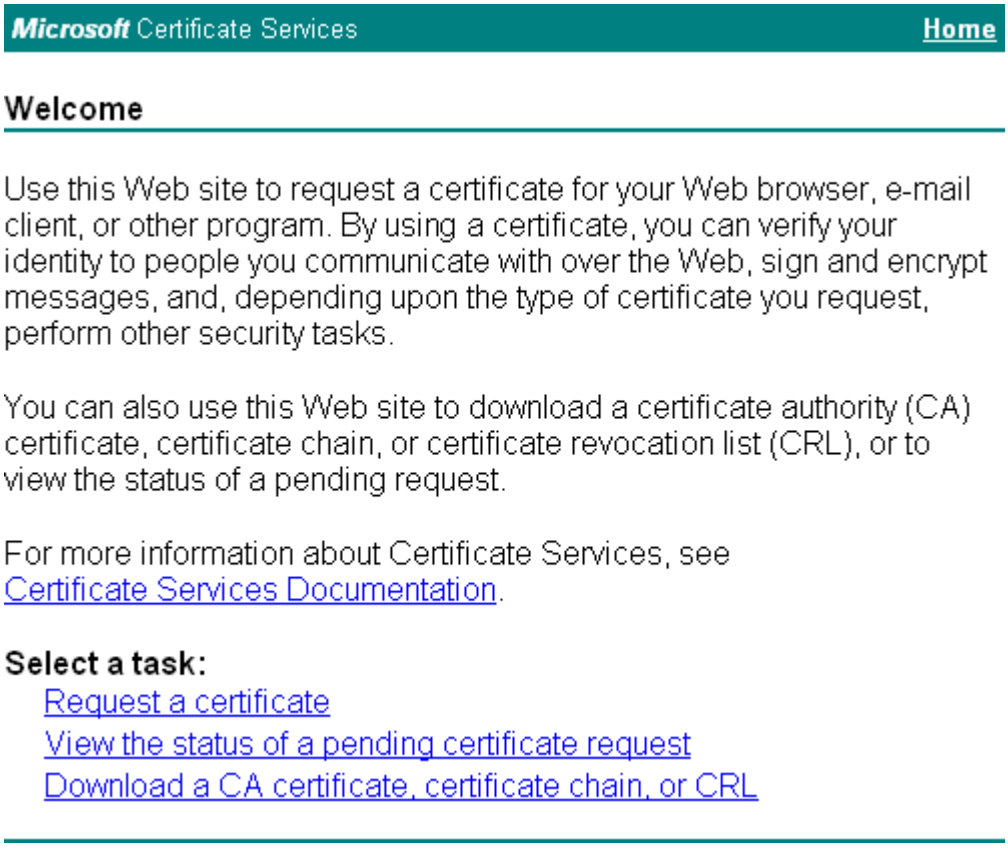
Generating a User Certificate

The easiest way to get the user certificate is to use a browser on a PC to navigate to the Certificate Authority.

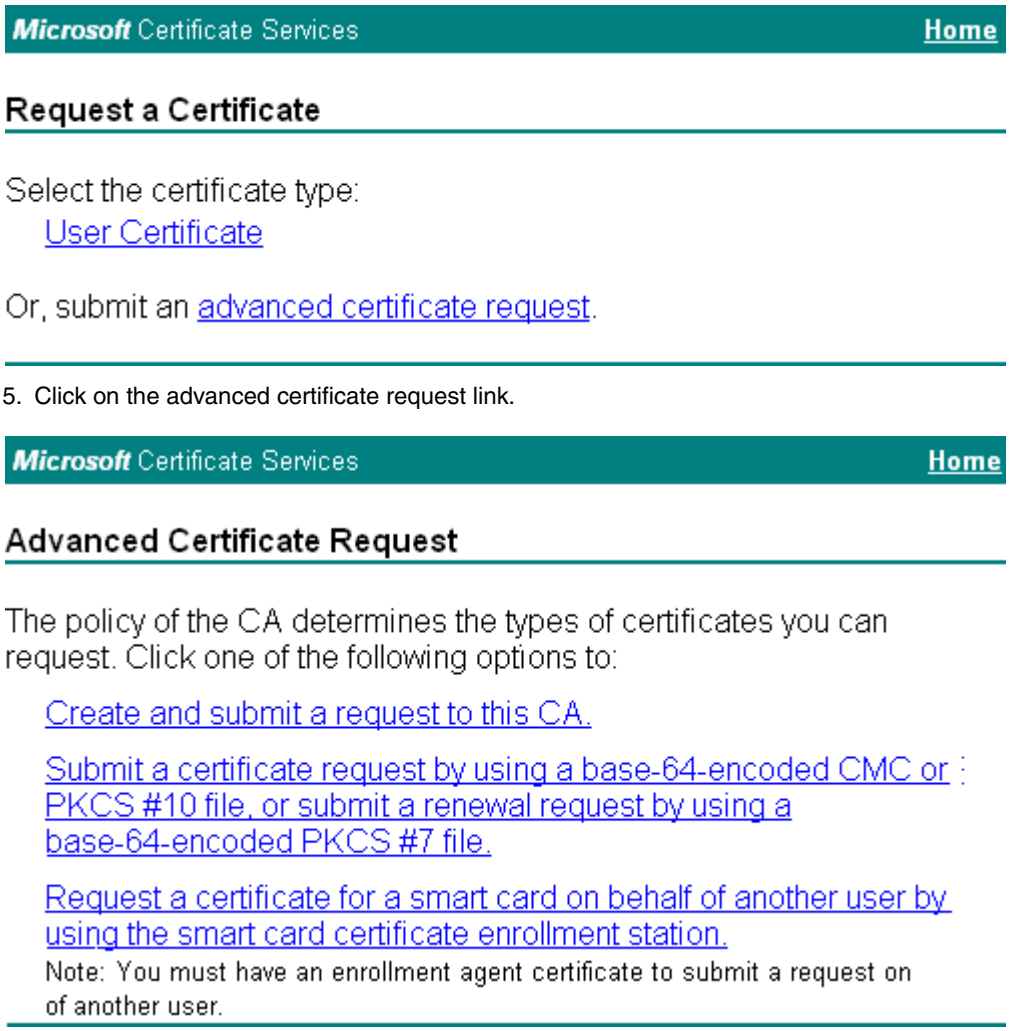
1. To request the user certificate, open a browser to http://<CA IP address>/certsrv.
2. Sign into the CA with the username and password of the person who will be logging into the mobile device.



3. This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the MX9 require the private key to be saved as a separate file rather than including the private key in the user certificate.


Microsoft Certificate Services
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

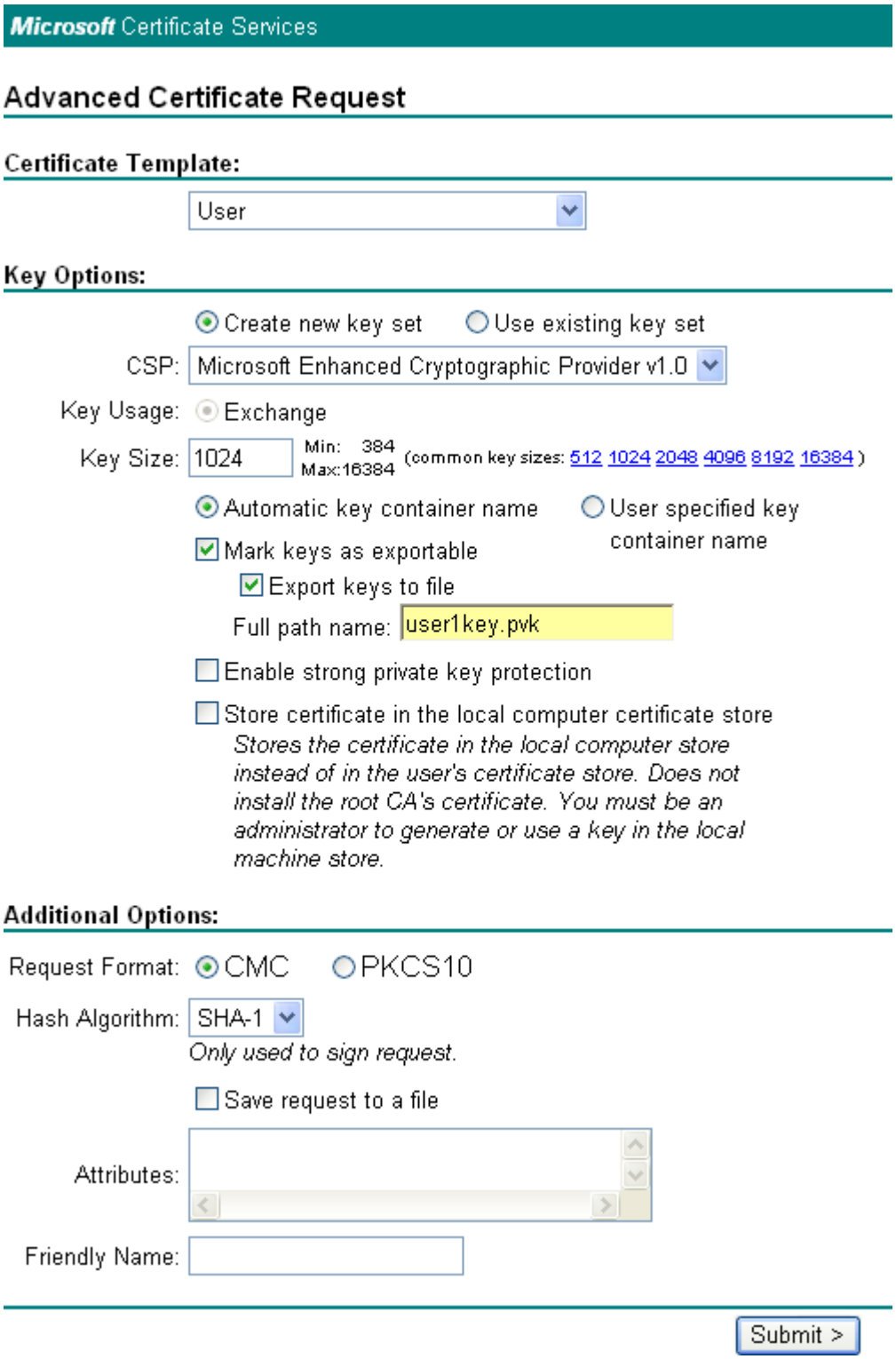
4. Click the Request a certificate link.



5. Click on the advanced certificate request link.

Microsoft Certificate Services
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on of another user.

6. Click on the Create and submit a request to this CA link.



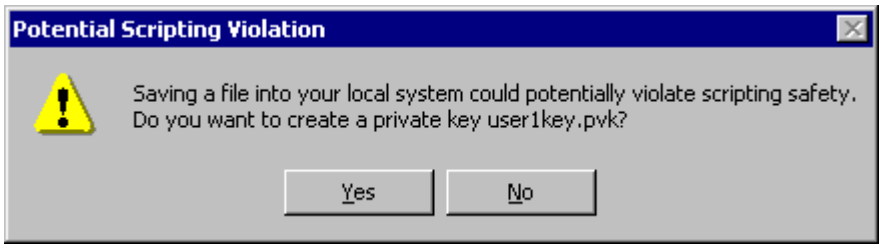
7. For the Certificate Template, select User.
8. Check the Mark keys as exportable and the Export keys to file checkboxes.

9. Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

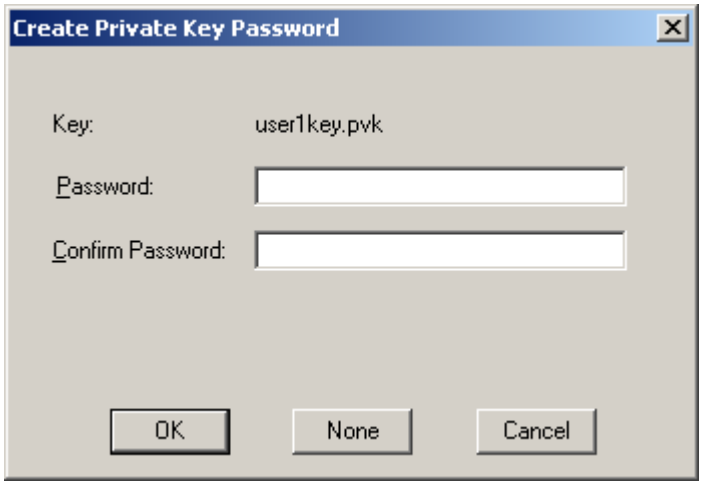
   Note: Be sure to note the name used for the private key file, for example EUSER.PVK. The certificate file created later in this process must be given the same name, for example, EUSER.CER.

10. DO NOT check to use strong private key protection.
11. Make any other desired changes and click the Submit button.

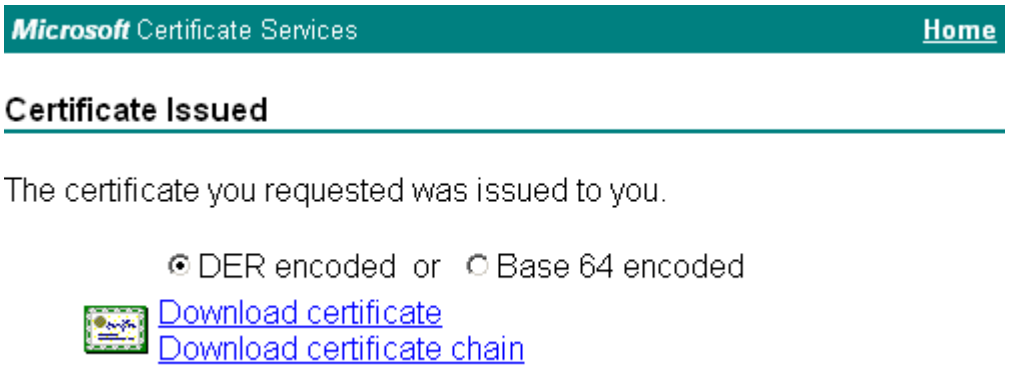

Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?
Yes
No


Potential Scripting Violation
Saving a file into your local system could potentially violate scripting safety.
Do you want to create a private key user1key.pvk?
Yes
No

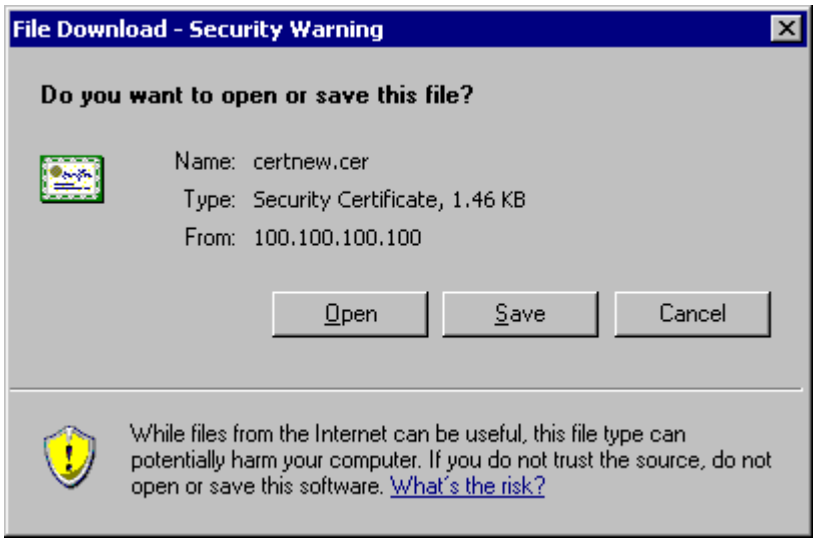
12. If any script notifications occur, click the “Yes button to continue the certificate request.



13. When prompted for the private key password:
    - Click None if you do not wish to use a password, or
    - Enter and confirm your desired password then click OK.



14. Click the Download certificate link.


File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.46 KB
From: 100.100.100.100
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

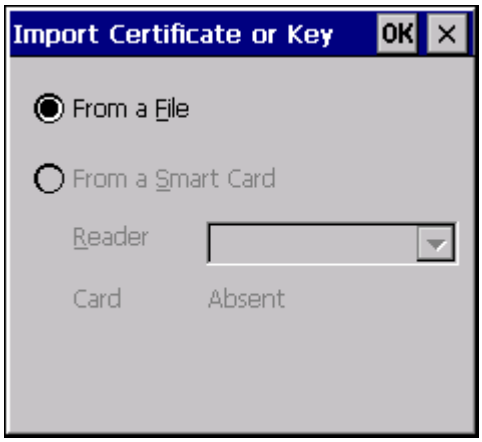
15. Click Save to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.
16. Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as EUSER.PVK then the certificate file created must be given the same name, for example, EUSER.CER.
17. Install the user certificate.

Installing a User Certificate

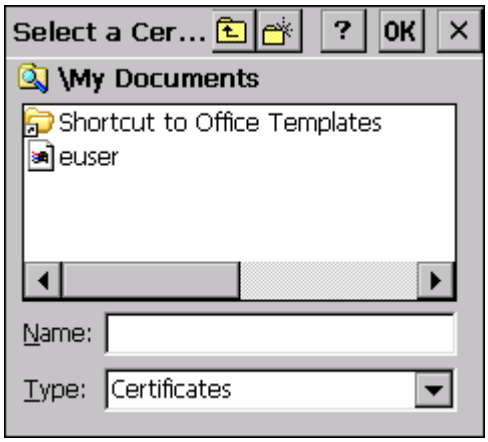
1. Copy the certificate and private key files to the MX9.
2. Import the certificate by navigating to **Start > Control Panel > Certificates**.
3. Select My Certificates from the pull down list.



4. Tap the Import button.



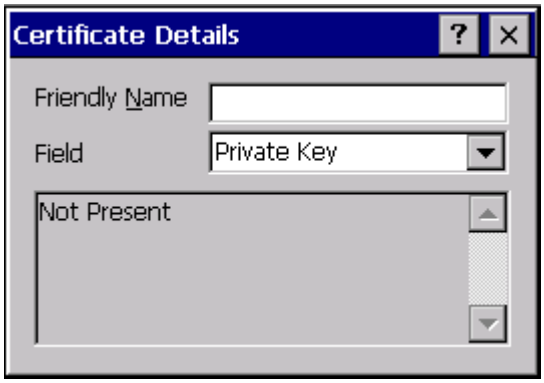
5. Make sure From a File is selected and tap **OK**.



6. Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.
7. The certificate is now shown in the list.



8. With the certificate you just imported highlighted, tap View.
9. From the Field pull down menu, select Private Key.



- If the private key is present, the process is complete.

- If the private key is not present, import the private key.

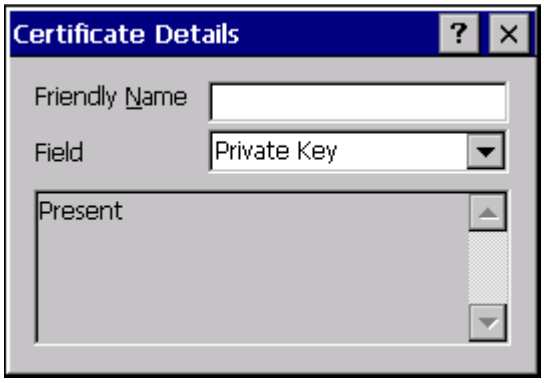
10. To import the private key, tap **OK** to return to the Certificates screen.
11. Tap import.



12. Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to Private Keys, select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Verify Installation

Tap on View to see the certificate details again.



The private key should now say Present. If it does not, there is a problem. Possible items to check:

Note: Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.

Note: Make sure the certificate and private key file have the same name, for example euser.cer for the certificate and euser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

11 KeyMaps

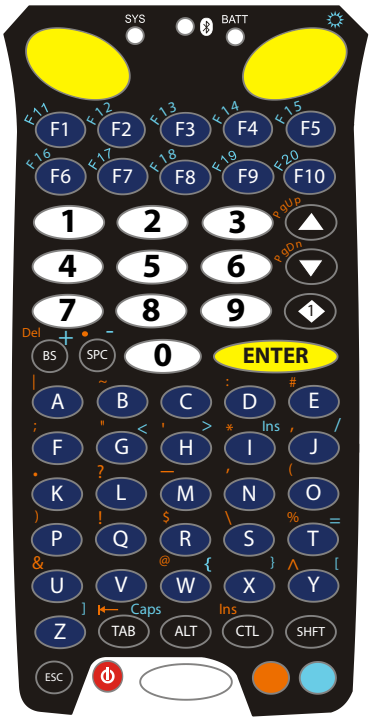
Introduction

The keypad is available in a 62-key or 38-key configuration. The 62-key keypad is also available in an IBM 5250 configuration.

- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- Sticky keys do not need to be held down while pressing the next (or desired) key.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Alphabetic keys default to lower case letters. Press the Shft key, 62 Key Keypad (page 2-4), or Shift key, 38 Key Keypad (page 2-5), then an alphabetic key for an uppercase letter.

Note: In general, sticky keys refer to those keys that, when pressed once and released, are still in effect and affect the function of the next key pressed.

62-Key Keypad KeyMap



The following keymap is used on an MX9 that is not running a Terminal Emulator. Terminal emulators use a separate keymap.

A modifier key pressed after itself toggles that modifier key off.

Modifier keys pressed following any other modifier key clears earlier modifier keys.

Any key press, other than the up arrow or down arrow, exits the volume control and backlight control.

To get this function	Press these keys in this order			Result / Notes
Windows key	CTL	ESC		Windows Start menu
On (when Off)	Power			Power On
Suspend toggle (when On)	Power			Suspend or Resume mode
Volume Up	Orange	Right Scan	Up Arrow	Volume increases
Volume Up	Blue	V	Up Arrow	Volume increases
Volume Down	Orange	Right Scan	Down Arrow	Volume decreases
Volume Down	Blue	V	Down Arrow	Volume decreases
Display Backlight Lighter	Blue	Right Scan	Up Arrow	Backlight lighter
Display Backlight Darker	Blue	Right Scan	Down Arrow	Backlight darker

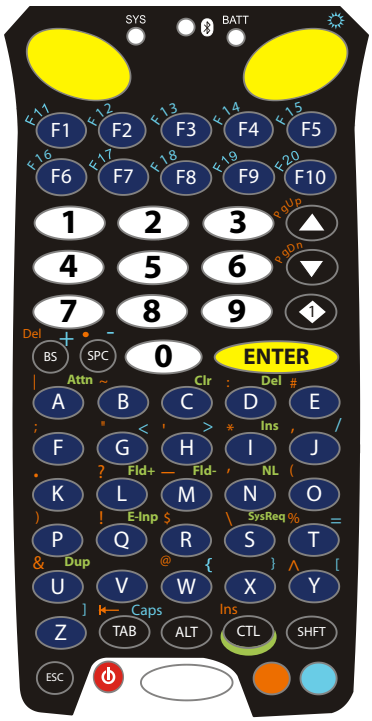
To get this function	Press these keys in this order			Result / Notes
Alt mode	ALT			Alt mode
Ctl mode	CTL			Control mode
Escape	ESC			Escape
Space	SPC			Space
Enter	Enter			Enter
Capslock toggle	Blue	TAB		Capslock is on or off
Mapped Diamond 1 Key	Diamond 1			Use the Keymap Control Panel to change default
Mapped Diamond 2 Key	Blue	Diamond 1		Use the Keymap Control Panel to change default
Uppercase Alpha toggle	SHFT			Shifted letter
Back space	BS (Backspace)			Back one space
Tab	TAB			Tab
Backtab	Orange	TAB		Backtab
Cursor Up	Up Arrow			Cursor up one line
Cursor Down	Down Arrow			Cursor down one line
Cursor Right	Blue	Up Arrow		Cursor right one space
Cursor Left	Blue	Down Arrow		Cursor left one space
Insert	Blue	I (letter i)		Insert mode
Insert	Orange	CTL		Insert mode
Delete	Orange	BS		Delete one character
Home	Orange	SHFT	Down Arrow	Home
End	Orange	SHFT	Up Arrow	End
Page up	Orange	Up Arrow		Up 1 screen
Page down	Orange	Down Arrow		Down 1 screen
F1	F1			F1 mode
F2	F2			F2 mode
F3	F3			F3 mode
F4	F4			F4 mode
F5	F5			F5 mode
F6	F6			F6 mode
F7	F7			F7 mode
F8	F8			F8 mode
F9	F9			F9 mode
F10	F10			F10 mode
F11	Blue	F1		F11 mode
F12	Blue	F2		F12 mode
F13	Blue	F3		F13 mode
F14	Blue	F4		F14 mode
F15	Blue	F5		F15 mode
F16	Blue	F6		F16 mode
F17	Blue	F7		F17 mode
F18	Blue	F8		F18 mode
F19	Blue	F9		F19 mode

To get this function	Press these keys in this order			Result / Notes
F20	Blue	F10		F20 mode
F21	SHFT	F1		F21 mode
F22	SHFT	F2		F22 mode
F23	SHFT	F3		F23 mode
F24	SHFT	F4		F24 mode
a	A			a (lowercase is the default)
b	B			b
c	C			c
d	D			d
e	E			e
f	F			f
g	G			g
h	H			h
i	I			i
j	J			j
k	K			k
l	L			l
m	M			m
n	N			n
o	O			o
p	P			p
q	Q			q
r	R			r
s	S			s
t	T			t
u	U			u
v	V			v
w	W			w
x	X			x
y	Y			y
z	Z			z
A	SHFT	A		A
B	SHFT	B		B
C	SHFT	C		C
D	SHFT	D		D
E	SHFT	E		E
F	SHFT	F		F
G	SHFT	G		G
H	SHFT	H		H
I	SHFT	I		I
J	SHFT	J		J
K	SHFT	K		K
L	SHFT	L		L
M	SHFT	M		M

To get this function	Press these keys in this order			Result / Notes
N	SHFT	N		N
O	SHFT	O		O
P	SHFT	P		P
Q	SHFT	Q		Q
R	SHFT	R		R
S	SHFT	S		S
T	SHFT	T		T
U	SHFT	U		U
V	SHFT	V		V
W	SHFT	W		W
X	SHFT	X		X
Y	SHFT	Y		Y
Z	SHFT	Z		Z
1	1			1
2	2			2
3	3			3
4	4			4
5	5			5
6	6			6
7	7			7
8	8			8
9	9			9
0 (zero)	0			0 (zero)
. (period)	Orange	SPC		Period
. (period)	Orange	K		Period
-	Blue	SPC		Dash or minus sign
/	Blue	J		Reverse Solidus or Backslash
\	Orange	S		Solidus or Forward slash
[	Blue	Y		Left square bracket
]	Blue	Z		Right square bracket
'	Orange	N		Acute accent or single quote or apostrophe
,	Orange	J		Comma
;	Orange	F		Semicolon
=	Blue	T		Equal sign
!	Orange	Q		Exclamation mark
!	SHFT	1 (number)		Exclamation mark
@	Orange	W		At sign
@	SHFT	2 (number)		At sign
#	Orange	E		Number sign
#	SHFT	3 (number		Number sign
$	Orange	R		Dollar sign
$	SHFT	4 (number)		Dollar sign
%	Orange	T		Percent sign

To get this function	Press these keys in this order			Result / Notes
%	SHFT	5 (number)		Percent sign
^	Orange	Y		Caret or circumflex
^	SHFT	6 (number)		Caret or circumflex
&	Orange	U		Ampersand
&	SHFT	7 (number)		Ampersand
*	Orange	I (alpha i)		Asterisk
*	SHFT	8 (number)		Asterisk
(	Orange	O (alpha o)		Left parenthesis
(	SHFT	9 (number)		Right parenthesis
)	Orange	P		Left parenthesis
)	SHFT	0 (zero)		Right parenthesis
"	Orange	G		Double quote
{	Blue	W		Curly left brace
}	Blue	X		Curly right brace
|	Orange	A		Vertical bar or Pipe
~	Orange	B		Tilde
<	Blue	G		Less than mark
>	Blue	H		Greater than mark
:	Orange	D		Colon
+	Blue	BS (Backspace)		Plus sign
?	Orange	L		Question mark
_	Orange	M		Underscore or horizontal bar
Enter	ENTER			Enter

62-Key 5250 Keypad Overlay KeyMap



To get this function	Press these keys in this order			Result / Notes
Attention (Attn)	CTL	A		5250 Attn
Clear (Clr)	CTL	C		5250 Clr
Delete (Del)	CTL	D		5250 Del
Duplicate (Dup)	CTL	U		5250 Dup
Erase Input (E-Inp)	CTL	Q		5250 E-Inp
Field Exit (Enter)	Diamond 1			5250 Field Exit
Fld - (Field Minus)	CTL	M		5250 Fld -
Fld + (Field Plus)	CTL	L		5250 Fld +
Ins (Insert)	CTL	I (capital i)		5250 Ins
NL (New Line)	CTL	N		5250 NL
SysReq (System)	CTL	S		5250 SysReq
The following are ANSI keymaps				
Windows key	CTL	ESC		Windows Start menu
On (when Off)	Power			Power On
Suspend toggle (when On)	Power			Suspend or Resume mode
Volume Up	Orange	Right Scan	Up Arrow	Volume increases
Volume Up	Blue	V	Up Arrow	Volume increases
Volume Down	Orange	Right Scan	Down Arrow	Volume decreases
Volume Down	Blue	V	Down Arrow	Volume decreases
Display Backlight Lighter	Blue	Right Scan	Up Arrow	Backlight lighter
Display Backlight Darker	Blue	Right Scan	Down Arrow	Backlight darker
Alt mode	ALT			Alt mode

To get this function	Press these keys in this order			Result / Notes
Ctl mode	CTL			Control mode
Escape	ESC			Escape
Space	SPC			Space
Enter	Enter			Enter
Capslock toggle	Blue	TAB		Capslock is on or off
Mapped Diamond 1 Key	Diamond 1			Use the Keymap Control Panel to change default
Mapped Diamond 2 Key	Blue	Diamond 1		Use the Keymap Control Panel to change default
Uppercase Alpha toggle	SHFT			Shifted letter
Back space	BS (Backspace)			Back one space
Tab	TAB			Tab
Backtab	Orange	TAB		Backtab
Cursor Up	Up Arrow			Cursor up one line
Cursor Down	Down Arrow			Cursor down one line
Cursor Right	Blue	Up Arrow		Cursor right one space
Cursor Left	Blue	Down Arrow		Cursor left one space
Insert	Blue	I (letter i)		Insert mode
Insert	Orange	CTL		Insert mode
Delete	Orange	BS		Delete one character
Home	Orange	SHFT	Down Arrow	Home
End	Orange	SHFT	Up Arrow	End
Page up	Orange	Up Arrow		Up 1 screen
Page down	Orange	Down Arrow		Down 1 screen
F1	F1			F1 mode
F2	F2			F2 mode
F3	F3			F3 mode
F4	F4			F4 mode
F5	F5			F5 mode
F6	F6			F6 mode
F7	F7			F7 mode
F8	F8			F8 mode
F9	F9			F9 mode
F10	F10			F10 mode
F11	Blue	F1		F11 mode
F12	Blue	F2		F12 mode
F13	Blue	F3		F13 mode
F14	Blue	F4		F14 mode
F15	Blue	F5		F15 mode
F16	Blue	F6		F16 mode
F17	Blue	F7		F17 mode
F18	Blue	F8		F18 mode
F19	Blue	F9		F19 mode

To get this function	Press these keys in this order			Result / Notes
F20	Blue	F10		F20 mode
F21	SHFT	F1		F21 mode
F22	SHFT	F2		F22 mode
F23	SHFT	F3		F23 mode
F24	SHFT	F4		F24 mode
a	A			a (lowercase is the default)
b	B			b
c	C			c
d	D			d
e	E			e
f	F			f
g	G			g
h	H			h
i	I			i
j	J			j
k	K			k
l	L			l
m	M			m
n	N			n
o	O			o
p	P			p
q	Q			q
r	R			r
s	S			s
t	T			t
u	U			u
v	V			v
w	W			w
x	X			x
y	Y			y
z	Z			z
A	SHFT	A		A
B	SHFT	B		B
C	SHFT	C		C
D	SHFT	D		D
E	SHFT	E		E
F	SHFT	F		F
G	SHFT	G		G
H	SHFT	H		H
I	SHFT	I		I
J	SHFT	J		J
K	SHFT	K		K
L	SHFT	L		L

To get this function	Press these keys in this order			Result / Notes
M	SHFT	M		M
N	SHFT	N		N
O	SHFT	O		O
P	SHFT	P		P
Q	SHFT	Q		Q
R	SHFT	R		R
S	SHFT	S		S
T	SHFT	T		T
U	SHFT	U		U
V	SHFT	V		V
W	SHFT	W		W
X	SHFT	X		X
Y	SHFT	Y		Y
Z	SHFT	Z		Z
1	1			1
2	2			2
3	3			3
4	4			4
5	5			5
6	6			6
7	7			7
8	8			8
9	9			9
0 (zero)	0			0 (zero)
. (period)	Orange	SPC		Period
. (period)	Orange	K		Period
-	Blue	SPC		Dash or minus sign
/	Blue	J		Reverse Solidus or Backslash
\	Orange	S		Solidus or Forward slash
[	Blue	Y		Left square bracket
]	Blue	Z		Right square bracket
'	Orange	N		Acute accent or single quote or apostrophe
,	Orange	J		Comma
;	Orange	F		Semicolon
=	Blue	T		Equal sign
!	Orange	Q		Exclamation mark
!	SHFT	1 (number)		Exclamation mark
@	Orange	W		At sign
@	SHFT	2 (number)		At sign
#	Orange	E		Number sign
#	SHFT	3 (number		Number sign
$	Orange	R		Dollar sign
$	SHFT	4 (number)		Dollar sign

To get this function	Press these keys in this order			Result / Notes
%	Orange	T		Percent sign
%	SHFT	5 (number)		Percent sign
^	Orange	Y		Caret or circumflex
^	SHFT	6 (number)		Caret or circumflex
&	Orange	U		Ampersand
&	SHFT	7 (number)		Ampersand
*	Orange	I (alpha i)		Asterisk
*	SHFT	8 (number)		Asterisk
(	Orange	O (alpha o)		Left parenthesis
(	SHFT	9 (number)		Right parenthesis
)	Orange	P		Left parenthesis
)	SHFT	0 (zero)		Right parenthesis
"	Orange	G		Double quote
{	Blue	W		Curly left brace
}	Blue	X		Curly right brace
|	Orange	A		Vertical bar or Pipe
~	Orange	B		Tilde
<	Blue	G		Less than mark
>	Blue	H		Greater than mark
:	Orange	D		Colon
+	Blue	BS (Backspace)		Plus sign
?	Orange	L		Question mark
_	Orange	M		Underscore or horizontal bar
Enter	ENTER			Enter

38-key Keypad KeyMap



The following keymap is used on an MX9 that is not running a Terminal Emulator. Terminal emulators use a separate keymap.

A modifier key pressed after itself toggles that modifier key off.

Any key press, other than a modifier key following any modifier key unsticks the modifier keys.

Any key press, other than up or down arrow, exits volume control mode or backlight control mode.

To get this function	Press these keys in this order			Result / Notes
Windows key	CTRL	Esc		Windows Start menu
On (when Off)	Power			Power On
Suspend toggle (when On)	Power			Suspend or Resume mode
Volume Up	Orange	Right Scan	Up Arrow	Volume increases
Volume Down	Orange	Right Scan	Down Arrow	Volume decreases
Display Backlight Lighter	Blue	Right Scan	Up Arrow	Backlight lighter
Display Backlight Darker	Blue	Right Scan	Down Arrow	Backlight darker
Scan (Right)	Right Scan			Activate decoder
Scan (Left)	Left Scan			Activate decoder
Alt mode	ALT			Alt mode
Ctrl mode	CTRL			Control mode
Escape	Esc			Escape
Space	SPC			Space
Enter	Enter			Enter
Capslock toggle	Blue	TAB		Capslock is on or off
Mapped Diamond 1 Key	Diamond 1			Use the Keymap Control Panel to change default
Mapped Diamond 2 Key	Diamond 2			Use the Keymap Control Panel to change default
Uppercase Alpha toggle	SHIFT			Shifted letter
Back space	BKSP			Back one space
Tab	TAB			Tab

To get this function	Press these keys in this order			Result / Notes
Backtab	Orange	TAB		Backtab
Cursor Up	Up Arrow			Cursor up one line
Cursor Down	Down Arrow			Cursor down one line
Cursor Right	Blue	Up Arrow		Cursor right one space
Cursor Left	Blue	Down Arrow		Cursor left one space
Insert	Orange	CTRL		Insert mode
Delete	Orange	BKSP		Delete one character
Home	Orange	SHIFT	Down Arrow	Home
End	Orange	SHIFT	Up Arrow	End
Page up	Orange	Up Arrow		Up 1 screen
Page down	Orange	Down Arrow		Down 1 screen
F1	F1			F1 mode
F2	F2			F2 mode
F3	F3			F3 mode
F4	F4			F4 mode
F5	F5			F5 mode
F6	F6			F6 mode
F7	F7			F7 mode
F8	F8			F8 mode
F9	F9			F9 mode
F10	F10			F10 mode
F11	Blue	F1		F11 mode
F12	Blue	F2		F12 mode
F13	Blue	F3		F13 mode
F14	Blue	F4		F14 mode
F15	Blue	F5		F15 mode
F17	Blue	F7		F17 mode
F18	Blue	F8		F18 mode
F19	Blue	F9		F19 mode
F20	Blue	F10		F20 mode
F21	SHIFT	F1		F21 mode
F22	SHIFT	F2		F22 mode
F23	SHIFT	F3		F23 mode
F24	SHIFT	F4		F24 mode
a	Alpha	2		a
b	Alpha	22		b
c	Alpha	222		c
d	Alpha	3		d
e	Alpha	33		e
f	Alpha	333		f
g	Alpha	4		g
h	Alpha	44		h
i	Alpha	444		i

To get this function	Press these keys in this order			Result / Notes
j	Alpha	5		j
k	Alpha	55		k
l	Alpha	555		l
m	Alpha	6		m
n	Alpha	66		n
o	Alpha	666		o
p	Alpha	7		p
q	Alpha	77		q
r	Alpha	777		r
s	Alpha	7777		s
t	Alpha	8		t
u	Alpha	88		u
v	Alpha	888		v
w	Alpha	9		w
x	Alpha	99		x
y	Alpha	999		y
z	Alpha	9999		z
A	SHFT	Alpha	2	A
B	SHFT	Alpha	22	B
C	SHFT	Alpha	222	C
D	SHFT	Alpha	3	D
E	SHFT	Alpha	33	E
F	SHFT	Alpha	333	F
G	SHFT	Alpha	4	G
H	SHFT	Alpha	44	H
I	SHFT	Alpha	444	I
J	SHFT	Alpha	5	J
K	SHFT	Alpha	55	K
L	SHFT	Alpha	555	L
M	SHFT	Alpha	6	M
N	SHFT	Alpha	66	N
O	SHFT	Alpha	666	O
P	SHFT	Alpha	7	P
Q	SHFT	Alpha	77	Q
R	SHFT	Alpha	777	R
S	SHFT	Alpha	7777	S
T	SHFT	Alpha	8	T
U	SHFT	Alpha	88	U
V	SHFT	Alpha	888	V
W	SHFT	Alpha	9	W
X	SHFT	Alpha	99	X
Y	SHFT	Alpha	999	Y
Z	SHFT	Alpha	9999	Z
1	1			1

To get this function	Press these keys in this order			Result / Notes
2	2			2
3	3			3
4	4			4
5	5			5
6	6			6
7	7			7
8	8			8
9	9			9
0 (zero)	0			0 (zero)
. (period)	Orange	SPC		Period
-	Blue	SPC		Dash or minus sign
/	Blue	1		Reverse Solidus or Backslash
\	Orange	1		Solidus or Forward slash
[	Orange	2		Left square bracket
[	Blue	2		Left square bracket
]	Orange	3		Right square bracket
]	Blue	3		Right square bracket
'	Orange	Alpha		Acute sign or single quote or apostrophe
,	Orange	6		Comma
;	Blue	0 (zero)		Semicolon
=	Orange	Esc		Equal sign
!	Blue	ALT		Exclamation mark
!	SHFT	1 (number)		Exclamation mark
@	Orange	5		At sign
@	SHFT	2 (number)		At sign
#	Orange	4		Number sign
#	SHFT	3 (number)		Number sign
$	Orange	9		Dollar sign
$	SHFT	4 (number)		Dollar sign
%	SHFT	5 (number)		Percent sign
^	Blue	CTRL		Caret or circumflex
^	SHFT	6 (number)		Caret or circumflex
&	SHFT	7 (number)		Ampersand
*	Orange	Diamond 1		Asterisk
*	SHFT	8 (number)		Asterisk
(	Blue	Esc		Left parenthesis
(	SHFT	9 (number)		Right parenthesis
)	Blue	SHIFT		Left parenthesis
)	SHIFT	0 (zero)		Right parenthesis
"	Blue	Alpha		Double quote
{	Blue	4		Curly left brace
}	Blue	5		Curly right brace
|	Orange	ALT		Vertical bar

To get this function	Press these keys in this order			Result / Notes
~	Blue	9		Tilde
<	Blue	7		Less than mark
>	Blue	8		More than mark
:	Orange	0 (zero)		Colon
+	Blue	BKSP (Backspace)		Plus sign
?	Orange	8		Question mark
_	Orange	7		Underscore or horizontal bar

12 Battery Charger

Unpacking your Battery Charger

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Introduction

The MX9 Battery Charger is designed to simultaneously charge four rechargeable Lithium Ion (Li-Ion) battery packs. The time required for charging is dependent upon the battery pack temperature and conditions.

The battery charger should be located in an area where it:

- Is well ventilated.
- Is not in high traffic areas.
- Locates or orients the AC cord so that it will not be stepped on, tripped over or subjected to damage or stress.
- Has enough clearance to allow easy access to the power port on the back of the device.
- Is protected from rain, dust, direct sunlight or inclement weather.

This device is intended for indoor use only and requires an indoor AC power source. The charger is not approved for use in hazardous locations.

This device cannot charge/recharge coin cell batteries sealed inside the mobile device, if any.

This chapter is intended to familiarize the user with the safety and operating instructions necessary to use the MX9 Battery Charger (Model MX9385CHARGER, MX9384CHARGER) to charge rechargeable lithium-ion battery packs (MX9380BATTERY, MX9381BATTERY).

This information should be readily available to all users and maintenance personnel using this battery charger.

Store the charger and batteries (when not in use) in a cool, dry, protected place.

Cautions and Warnings

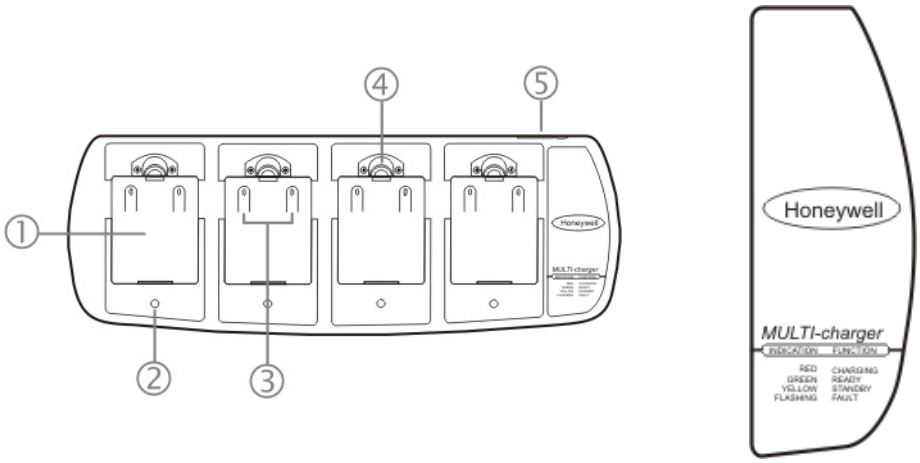
Battery Charger

- There is a risk of explosion if the MX9 Li-Ion battery in the charging pocket is replaced by an incorrect type. Other batteries or battery packs may burst causing injury or property damage.
- Do not insert any other type of Li-Ion battery in the MX9 battery charging pocket.
- Do not allow cleaning agents of any kind to contact the battery charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.
- Disconnect the charger from AC power by pulling the plug; not the cord.
- Use care when inserting battery. Do not “slam” or slide the battery into the pocket, this could damage the charger.
- Keep dirt and foreign objects out of the battery pocket. Do not short circuit any of the contacts in the battery pocket, this could result in injury or property damage.
- Do not disassemble or perform modifications to the charger. There are no user serviceable components in the charger.

Lithium-Ion Battery Pack

- Dispose of used Li-Ion batteries according to the instructions for the type of battery.
- When not in use, lay the battery pack contact-side up in a protected environment.
- Do not store the Li-Ion battery pack in direct sunlight or anywhere the battery pack cannot cool down.
- If the Li-Ion battery pack is hot after removal from the MX9, allow it to cool at room temperature or in a cool air stream before placing it in the charger.
- Do not dispose of Li-Ion batteries into a fire. Burning will generate hazardous vapors and may cause the battery to explode. Failure to observe this warning may result in injury from inhalation of vapors or burns from flying debris.
- Do not immerse Li-Ion batteries in water or any other liquid. If batteries are immersed, contact Honeywell.
- Do not disassemble or perform modifications to the battery. There are no user serviceable components in the battery.
- Do not place the Li-Ion battery into a pocket or toolbox with conductive objects (coins, keys, tools, etc.). A Li-Ion battery placed on damp ground or grass could be electrically shorted.
- Do not store Li-Ion batteries above 140°F (60°C) for extended periods.
- Failure to observe these warnings could result in injury or damage to the battery from rapid discharge of energy or battery overheating.
- Electrolyte Burns. Be careful when handling batteries. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it! Lead and Nickel-based cells contain a chemical solution that burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.
- Electrical Burns. Batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a charged battery in a pocket or case with keys, coins, or other metal objects.

Front View



1. Battery Charging Pocket
2. Battery Charging Pocket LED
3. Battery Pocket Spring Clip
4. Battery Retaining Clip
5. AC Power port

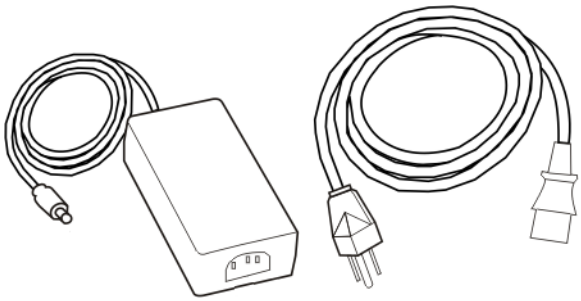
Installation

Assemble the Power Supply

Assemble the AC adapter for the MX9 Battery Charger before connecting it to the charger.

The AC power supply for the battery charger is shipped with the battery charger. Contact Customer Support (page 15-1) if there is no AC cable.

The battery charger power supply is intended for use with the MX9 battery charger *only.*



1. Plug the 3-prong end of the cable into an AC wall outlet.
2. Firmly press the female end of the power cable into the male connector on the AC power adapter. An LED on the power adapter illuminates when AC power is available.
3. AC power is now being applied to the power adapter.

Setup

Place the battery charger on a flat, horizontal, hard surface or fasten securely to a stable surface using the keyhole openings on the bottom of the battery charger. See Mounting.

Do not insert battery packs until the battery charger has finished powering up:

1. Assemble the Power Supply and connect it to an indoor power source (e.g., wall outlet).
2. Insert the power connector from the power supply into the power outlet at the back of the battery charger.
3. AC power is now being applied to the battery charger and it begins to power up.
4. Charge pocket LEDs flash while the battery charger enters and exits the startup check.
5. When the charge pocket LEDs are not illuminated, the battery charger is ready for use.

Mounting

The battery charger should be located in an area where it:

- Is well ventilated.
- Is not in high traffic areas.
- Locates or orients the AC cord so that it will not be stepped on, tripped over or subjected to damage or stress.
- Has enough clearance to allow easy access to the power port on the back of the device.
- Is protected from rain, dust, direct sunlight or inclement weather.

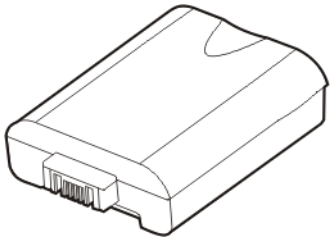
This device is intended for indoor use only and requires an indoor AC power source. The charger is not approved for use in hazardous locations.

Place the battery charger on a flat, horizontal, hard surface.

The battery charger can be mounted to a stable, vertical surface (e.g., wall) using the keyhole openings in the bottom panel of the battery charger.

Care should be taken, when inserting batteries in a vertical-mounted battery charger, that the battery is secured by the latch in the battery charging pocket.

Charging Batteries



New batteries should be charged fully before first use. The life and capacity of a Lithium Ion battery pack can vary significantly depending on the discharge current and the environment in which it is used.

When a battery is placed in a charging pocket, the battery charger begins charging the battery. There is a slight delay while the charger evaluates the condition of the battery (ambient temperature, remaining charge, etc.) before charging begins.

As with all batteries, expect to see a reduction in the total number of operations a fully charged battery pack can deliver as it ages. When the battery reaches end of life (end-of-life occurs after 500 charge/discharge cycles) it must be replaced.

Battery packs do not need to be fully discharged between charge cycles.

While charging, the charger and battery pack will generate enough heat to feel warm. This is normal and does not indicate a problem.

Inserting a Battery into the Charging Pocket



It is important that battery packs are inserted into the charging pocket correctly. Inserting the battery incorrectly could result in damage to the battery pack or the charger.

Do not “slam” the battery pack into the charging pocket. Damage may result.

1. When preparing the battery pack for insertion into the battery charging pocket, hold the battery with its four charging contacts in line with the charging contacts in the charging pocket.
2. Aim the retaining catch towards the back of the charger.
3. Push the locking tab towards the back of the battery charging pocket until it stays in place.
4. Place the battery in the charging pocket, making sure the tab at the top of the battery pack fits into the slot at the top end of the charging pocket.
5. With a hinging motion, slip the battery down into the charging pocket until the locking tab clicks into place and the battery pack is secure in the charging pocket.

Removing the Battery from the Charging Pocket

1. Push the locking tab away from the battery. The battery will pop up slightly.
2. Grasp the battery and with a hinging motion, lift it out of the charging pocket.

Interpreting the Charging Pocket LEDs

The status of the charge operation is indicated by the color of the LED for each charging pocket.

RED Continuous - on any charge pocket

Continuous red means the battery pack is charging.

RED FLASHING - on all charge pockets

Battery charger fault or failure.

GREEN - on any charge pocket

Continuous green means the battery pack charge is complete - Battery is Ready.

YELLOW - on any charge pocket

Continuous yellow / amber means the battery pack temperature is out of range. The charging pocket is in standby mode while the pocket waits for the battery pack to warm up or cool down.

NO LIGHT - on any charge pocket

No light on a charge pocket means there is no battery pack installed ,

- or the battery pack in the pocket is not fully inserted,
- or a defective or damaged battery pack is installed,
- or the charger is defective or damaged. Refer to Battery Charger Help (page 12-6).

NO LIGHT - on all charge pockets

No light means there is no AC power available for the battery charger or there is power but there are no batteries in any charging bay.

Battery Charger Help

The following is intended as an aid in determining whether the battery pack or the charger may be malfunctioning:

Issue	Cause	Solution
Battery pack does not fit in charging pocket.	Different manufacturer's battery pack, or there is an object in the charging pocket.	Check if the MX9 battery pack has Honeywell part number MX9380BATT or MX9381BATT (Low Temperature) on the label. If not, do not use. Remove the object from the charging pocket.
No battery pack in charger, but any of the LEDs are on.	Dirt or foreign objects are in the charging pocket.	Unplug charger from AC supply. Remove any dirt or foreign objects from the charging pocket. If the LEDs continue to remain ON, the charger may be defective. Return charger to an authorized Honeywell service center.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Battery pack is not making contact with battery charge terminals in the charging pocket.	Push battery pack in firmly. Do not “slam” the battery pack into the charging pocket.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Faulty battery pack.	Replace battery pack.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	New battery pack, same result.	Contact Customer Support (page 15-1) for replacement options.
When you first put a fully charged battery pack in the charging pocket, the RED LED comes on, indicating the battery pack is charging.	During the first few minutes, the battery charger checks the battery pack for correct voltage and charge state. During this time the LED is RED and is continuously ON. After charging is complete, the LED is GREEN.	There is nothing wrong with the battery pack or charger. Do not “top off” a fully charged battery pack by repeatedly placing it in the charging pocket. The battery pack may overheat and be damaged.
LED is flashing RED at any pocket.	Current could not be sourced through the battery pack due to age, exhaustion or damage to the cell(s). The battery pack does not communicate with the charger.	Contact Customer Support (page 15-1) for battery pack replacement options.
LED is flashing RED at any pocket.	The charger’s timeout period has expired.	Make sure that the battery pack temperature is within specification and retry charging. Contact Customer Support (page 15-1) if problem repeats, for battery pack replacement options.

Issue	Cause	Solution
LED is flashing RED at any pocket.	The battery pack voltage has not reached 6.0V within 30 minutes and the charger has timed out.The battery pack voltage has not reached 2.5V within 60 minutes and the charger has timed out.	Contact Customer Support (page 15-1) for battery pack replacement options.
Solid YELLOW / AMBER LED when battery pack is inserted in the charging pocket.	The battery pack is too hot or too cold to charge.	Remove battery pack from the charging pocket and allow it to adjust to room temperature. *Note: If the battery pack is left in the charging pocket, it will cool down or warm to a temperature upon which the charger will begin the charge cycle. However, depending on the temperature of the battery, it may take 2-3 hours to adjust. The cool-down / warm-up of a battery pack is much quicker if the battery is not in the charging pocket.*

Charger Cleaning, Storage and Service

Cleaning

Unplug the charger from the power source before cleaning or removing debris from charging pockets.

Use only mild detergent with a slightly damp cloth to clean the outside of the charger. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Remove all batteries from the charging bays and disconnect AC power before placing the charger in storage. It should be stored in a cool, dry place, protected from weather and airborne debris.

Battery packs should be kept in a cool, dry place whenever possible. Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down. Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Service

There are no user serviceable parts in the Rechargeable Lithium Ion Battery or the Charger. Contact Customer Support (page 15-1) should your charger require service.

Battery Cleaning, Storage and Service

Cleaning

The battery pack should not require cleaning unless it has become heavily soiled. Old or damaged batteries should be disposed of promptly and properly. The best way to dispose of used batteries is to recycle them. Battery recycling facilities recover the Nickel, Lithium or Lead from old batteries to manufacture new batteries.

Use only mild detergent with a slightly damp cloth to clean the outside of the battery. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Battery packs should be stored, charging contact side up, in a cool dry place, protected from weather and airborne debris, whenever possible.

Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down.

Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Note: Battery packs may leak up to 1 mA current through the battery contacts when left in a non-powered charger pocket.

Service

There are no user serviceable parts in the Lithium Ion Battery Pack. Contact Customer Support (page 15-1) for battery disposal and replacement options.

13 Cradles

Unpacking your Cradles

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Communication cables and power cables are ordered separately.

Overview

This chapter provides instruction for the end-user, installer or system administrator to follow when setting up or using MX9 cradles.

Two cradles are available:

- A desktop cradle that secures the MX9, recharges batteries and enables communications between the MX9 and another device. See Using a Desktop Cradle (page 13-3).
- A powered vehicle-mount cradle that secures the MX9, isolates it from shock and vibration and recharges the battery. See Using a Powered Vehicle Cradle (page 13-11).

MX9 cradles are not certified for use in hazardous locations.

The MX9 must have a main battery installed when it is docked in a cradle. Wireless host/client communications can occur whether the cradle is receiving external power or not as wireless functions draw power from the main battery in the MX9.

MX9 keypad data entries can be mixed with cradle-tethered scanner bar code data entries while the MX9 is in a powered cradle. Bluetooth device connection and use, while the MX9 is docked, are managed by the MX9 Bluetooth program, not the cradle.

The MX9 can be either On, Off or in Suspend Mode while in the cradle. Special purpose and power cables are available from Honeywell.

Never put the MX9 into a vehicle mounted assembly until the assembly is securely fastened to the vehicle.

Preparing the Cradle for Use

Note: Keep dirt and foreign objects out of the cradle. Do not short circuit any of the charging terminals (pins), as this action could result in injury or property damage.

Place cradles on a stable surface out of the way of:

- inclement weather,
- extremely high concentrations of dust or wind blown debris,
- accidental knocks, bumps or other shocks to the cradle and items in the cradle bays.
- Leave enough space at cable connectors to ensure cables are protected from jostling, tugging or being disconnected by passing objects.

In addition to the above, vehicle mounted cradles should be positioned in the vehicle where the cradle:

- is protected from rain and inclement weather,
- does not obstruct the driver's vision or safe vehicle operation,
- can be easily accessed by a user seated in the driver's seat while the vehicle is not in operation.
- Leave enough space at the back of the cradle for the MX9 trigger handle.
- There must be at least 2” clearance at the back of the vehicle cradle for power, serial interface and the Input/Output cables.

Tethered Scanners and the MX9 Cradles

An MX9 powered cradle supports tethered scanner attachment. A powered cradle provides 5V power to a tethered scanner. The passive vehicle cradle cannot support tethered scanner attachment. There is no software in the cradles.

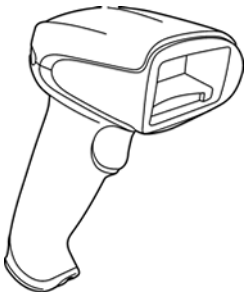
Note: Tethered scanners connect to powered cradles by USB or serial connection.

Note: Pressing the MX9 Scan button has no effect on tethered bar code scanners connected to a powered cradle. Tethered scanners read bar code scans only when the trigger on the tethered scanner is pressed.

A tethered scanner can be connected to the 9-pin RS232 Serial Interface port on the desktop cradle or to the Serial Interface port on the back of the vehicle cradle.

Bluetooth scanner connection and use, while the MX9 is docked in a cradle, are managed by the MX9 Bluetooth client, not the cradle.

MX9 keypad data entries can be mixed with tethered scanner bar code data entries. Any tethered scanner that decodes the bar code internally and outputs an RS232 data stream may be used. It sends the data to the MX9 in ASCII format.



Tethered scanners send scanned data to the MX9 when the MX9 is in a powered cradle and the tethered scanner is connected to the Serial Interface port on the cradle.

When a tethered scanner is connected to the Serial Interface port on a powered cradle, the MX9 must be configured as follows:

1. Open the Data Collection Wedge Main tab panel on the MX9.
2. Enable either Port 1, Port 2 or Port 3.
3. Close the Data Collection Wedge application.

Cradle Cleaning, Storage and Service

Cleaning

Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the surfaces and/or battery connectors.

Use a clean soft cloth to wipe any dirt, moisture or grease from the MX9, charging contacts or the cradle. Do not use any liquid to clean the cradle, battery pack, MX9, or charging terminals (pins). Spray or dampen the cleaning cloth with liquids/sprays. If possible, clean only those areas which are soiled.

Lint/particulates can be removed from the connectors, charging terminals and charging/docking bays with clean, filtered canned air.

Storage

When the cradle is not in service, it should be stored in a cool dry place, protected from weather and airborne debris. Do not store a spare MX9 or spare battery in the cradle in storage.

Service

There are no serviceable parts in MX9 cradles. Do not attempt to open the units.

If the cradle or mounting components are broken, loose or cracked, the assembly must be taken out of service and replaced. Periodically test a mounted cradle for stability and tighten connections as needed.

Battery Cleaning, Storage and Service

Cleaning

The battery pack should not require cleaning unless it has become heavily soiled. Old or damaged batteries should be disposed of promptly and properly. The best way to dispose of used batteries is to recycle them. Battery recycling facilities recover the Nickel, Lithium or Lead from old batteries to manufacture new batteries.

Use only mild detergent with a slightly damp cloth to clean the outside of the battery. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Battery packs should be stored, charging contact side up, in a cool dry place, protected from weather and airborne debris, whenever possible.

Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down.

Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Battery packs may leak up to 1 mA current through the battery contacts when left in a non-powered charger pocket.

Service

There are no user serviceable parts in the Lithium Ion Battery Pack. Contact Technical Assistance (page 15-1) for battery disposal and replacement options.

Using a Desktop Cradle

Introduction

Note: When an external power supply is used to power this cradle, the external power supply should be UL Listed, with LPS or Class 2 outputs rated 12V, minimum 2 amps.

The desktop cradle is available in three configurations:

1. Without a power supply. A power supply must be ordered separately.
2. With a power supply and a US power cord.
3. With a power supply but without a power cord. A country specific power cord must be provided.

Communications cables for the MX9 are available separately.

Quick Start - Desktop Cradle

The following list outlines, in a general way, the process to follow when preparing the MX9 desktop cradle for use. Refer to the following sections in this document for more details.

1. Connect the cradle end of the power adapter cable to the Power port on the back of the cradle.
2. Attach the AC power connector to a dependable power source.
3. Attach any desired external cabled devices to the ports on the cradle.
4. The desktop cradle is ready for use.

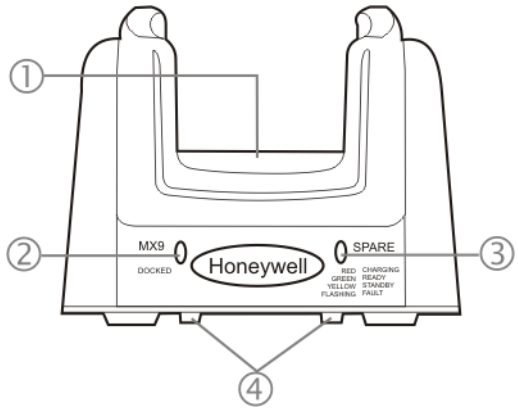
Battery Charging in a Desktop Cradle

Main battery recharging in a docked MX9 is managed by the Power Management settings in the MX9. Refer to the Power control panel on the MX9.

The spare battery in the spare battery well re-charges with or without an MX9 in the dock. The spare battery is fully charged in approximately four hours.

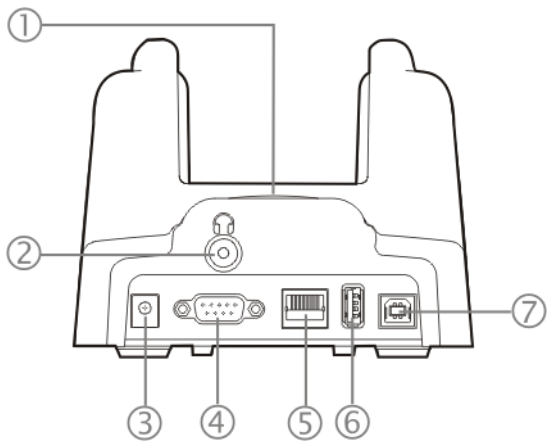
The cradle must be receiving power from an external power source before the main battery in the docked MX9 or spare battery pack charging can take place.

Front View



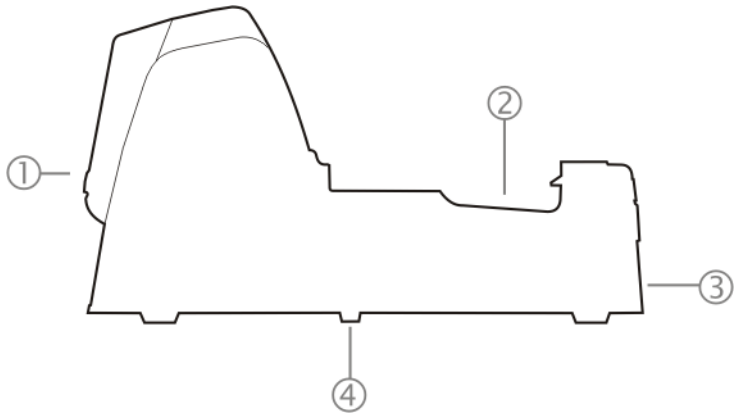
1. MX9 Cradle Docking/Charging Bay
2. MX9 Docked LED
3. Spare Battery LED
4. Table Mounting Holes

Back View



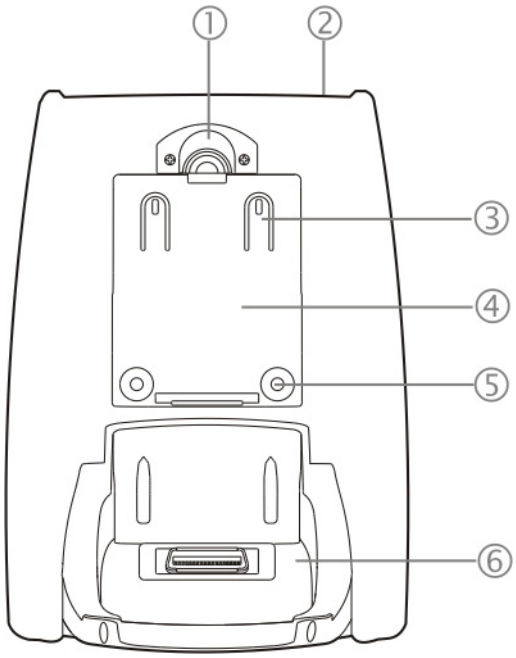
1. Spare Battery Charging Bay
2. Headset Audio Cable port
3. AC/DC Power port
4. Serial port
5. Ethernet port
6. USB Client port
7. USB Host port

Side View



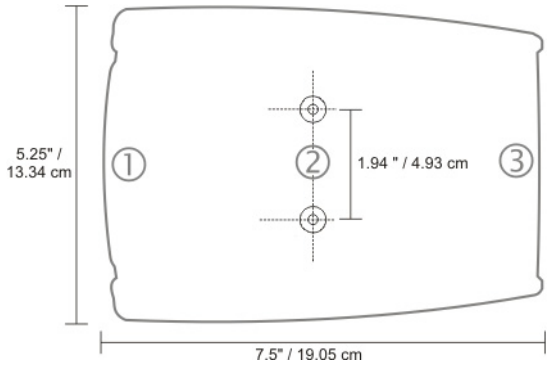
1. Front / MX9 Docking/Charging Bay
2. Spare Battery Charging Bay
3. Back / Power port
4. Table Mounting Holes

Top View



1. Spare Battery Charging Bay Battery Catch
2. Power port
3. Spare Battery Spring
4. Spare Battery Charging Bay
5. Desktop Table Mounting Holes
6. MX9 Docking/Charging Bay

Desktop Mounting Footprint



1. Front
2. Table Mounting Hole Guides
3. Back

Not to Scale

Bolts, washers, screws, screwdriver or wrench needed when attaching the MX9 desktop cradle to a protected flat surface are not supplied by Honeywell.

Periodically check the table mounting hardware and re-tighten if necessary. Table mounting hardware can be finger-tightened.

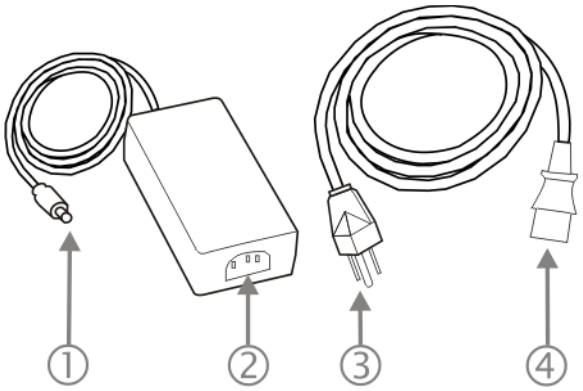
Note: Do not over-tighten the table mounting hardware. If the cradle is cracked, it must be replaced before being placed into service.

Assemble/Attach the AC Power Adapter

Note: Connect the cable to the cradle first, then to an AC source.

The external Power Supply for the cradle is shipped with the cradle. Contact Technical Assistance (page 15-1) if there is no AC cable.

The Power connector is located on the back of the cradle.



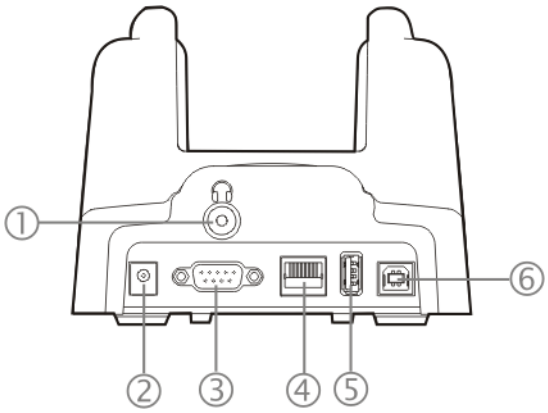
1. Plug the AC power plug (3) into any AC wall outlet with a dependable power source.
2. Firmly press the adapter end (4) of the power cable into the 3 pin connector (2) on the power adapter.
3. Firmly press the cradle end (1) of the power cable into the power port on the back of the cradle.
4. AC power is now being supplied to the AC power adapter and the cradle.

Connecting Input/Output and Power Cables to the Desktop Cradle

Note: Route all cables to ensure they are protected from jostling, tugging or being disconnected by passing objects.

The cradle must be receiving power from an external power source before MX9 battery charging can begin.

Note: Periodically test the connections for stability and adjust as necessary.



1. Headset Audio port
2. Power port
3. Serial (RS232) port
4. Ethernet port
5. USB Client port
6. USB Host port

Desktop Cradle Connector Identifiers

2 - Power	3 - Serial	4 - Ethernet	5,6 - USB A and USB B

Connecting a Headset Audio Cable

Firmly press the cradle end into the MX9 Headset Audio port (1) on the back of the cradle. Test the connection for stability.

Connecting the Power Cable

Assemble the power cable by first plugging the AC end into an electric socket, then plug the other end into the AC adapter. The cradle cord is secured to the AC adapter. Firmly press the cradle end of the power cable into the MX9 Power port (2) on the back of the cradle. Test cable connections for stability.

Connecting a Serial Cable

The serial cable is connected to the Serial port (3) on the back of the desktop cradle. The serial cable end can originate with a tethered scanner, a desktop/laptop PC, a printer or another serial device.

Align the RS232 serial cable end (female) carefully to the Serial Interface port (male) on the back of the desktop cradle. Press the ends together and finger tighten the screws on either side of the connector. Test the connection for stability.

Connecting an Ethernet RJ-45 Cable

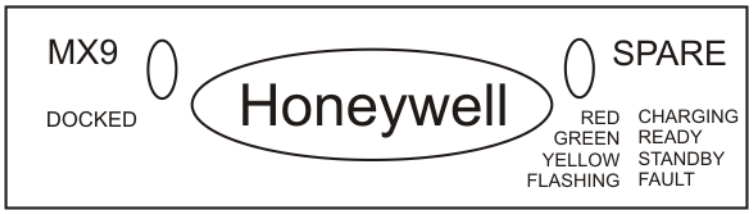
Firmly press the cradle end into the MX9 Ethernet RJ-45 port (4) connector on the back of the cradle until it clicks into place. Test the connection for stability.

Connecting a USB Host and USB Client Cable

Firmly press the cable end into the MX9 USB Client (5) or USB Host (6) Port connector on the back of the cradle. Test the connections for stability.

Cradle LEDs

When the desktop cradle AC/DC power supply cable begins to supply power to the cradle, the cradle LEDs flash yellow, red, green for three seconds then turn off. The cradle is ready for use.



Docked LED

When Docked LED is …	It means ….
Off	MX9 not inserted or no power applied
Red	MX9 docked and power applied.

Note: The cradle must be connected to a AC power before the LEDs illuminate.

Spare Battery LED

When Spare LED is …	It means ….
Off	Battery pack not inserted or no power applied
Green	Battery pack fully charged
Red	Battery pack charging
Yellow / Amber	Battery pack temperature out of range
Flashing Red	Battery pack fault or failure

Note: Spare battery charging does not require an MX9 be docked in the docking bay.

MX9 System Status LED Status when Docked

The MX9 System Status LED is located at the top of the keypad.

When the LED is . . .	The Status is . . .	Comment
Blinking Red	Power Fail	Replace the main battery with a fully charged main battery. Or Connect the MX9 to external AC power to allow the internal charger to charge the main battery e.g., dock in a powered cradle.
Steady Red	Main Battery Low	Low Battery Warning. Replace the main battery with a fully charged main battery. Or dock the MX9 in a powered cradle.
Blinking Green	Display Off	No user intervention required.
No Color	Good	No user intervention required.

Docking and Undocking the MX9

When the MX9 is in Suspend Mode it wakes up when it is docked in a powered cradle. There is no change in mode state settings or behavior when the MX9 is docked in a cradle without a power source.

MX9 mode states while the MX9 is in a powered cradle e.g., suspend, resume, display backlight, etc., are managed by the MX9 OS Power settings.

If the cradle is not permanently attached to the work surface, stabilize the cradle with one hand while inserting or removing the MX9 with the other hand.

The MX9 is inserted into the charging pocket with the keypad facing forward.

Dock the MX9

Remove any cables attached to the I/O port in the base of the MX9.

Carefully press the MX9 straight down into the docking bay until the multi-pin connector at the base of the MX9 clicks into place with the multi-pin charging/communication connector at the bottom of the docking bay. The MX9 cradle is designed to secure the MX9 facing front.

The cradle's Docked LED illuminates.

Undock the MX9

Remove the MX9 from the cradle by pulling it straight up and out of the docking bay. If necessary, brace the cradle with one hand while the other hand removes the MX9.

The cradle's Docked LED turns Off.

Inserting / Removing a Spare Battery from the Desktop Cradle

Prerequisites: The steps outlined in Assemble/Attach the AC Power Adapter (page 13-6) have been completed and the cradle has a dependable power source. The cradle has been bolted to a stable surface, if desired.

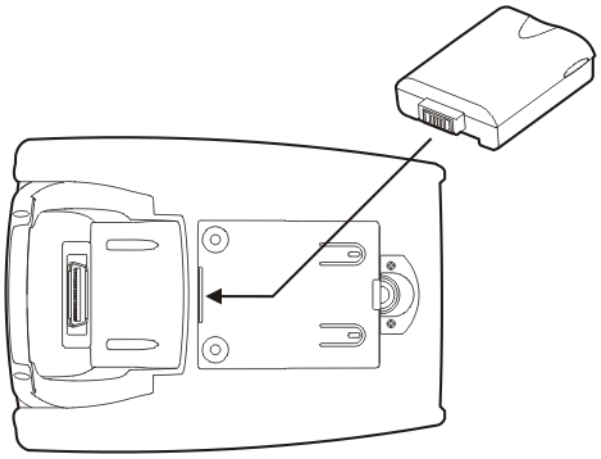
Note: Do not drop or slam the spare battery into the charging pocket. Damage may result.

A fully depleted spare battery recharges in approximately four hours in the MX9 powered cradle. Charging time may take longer if a tethered scanner, connected to the Serial port and drawing power from the cradle, is used.

The spare battery charger can recover a battery that has had its safety circuit tripped.

The spare battery well is molded in the shape of the MX9 main battery. The spare battery can be inserted in the battery well in only one direction. When there is an MX9, with or without a handle, docked in the cradle, a spare battery can still be inserted in the charging bay. You do not need to undock the MX9 before inserting or removing a Spare battery.

Stabilize the cradle with one hand when inserting/removing the spare battery, if necessary.



Inserting a Spare Battery

1. Hold the battery with the charging terminals facing down, toward the charging pocket.
2. Tilt the end (with the charging terminals) into the re-charging terminals at the front end of the spare battery charging bay. Slide the battery forward until it is fully inserted into the battery bay.
3. Push down on the spare battery until the catch clicks into place, securing the spare battery in the battery bay. This will ensure the charging contacts on the spare battery connect with the re-charging contacts in the battery bay.
4. The Spare charging bay LED illuminates indicating the battery is properly seated in the charging bay.

Removing a Spare Battery

A green Spare battery LED signifies the spare battery is charged.

Remove the Spare battery by sliding the latch in and pulling the Spare battery up, with a hinging motion, and out of the charging bay. The Spare charging bay LED turns Off.

Desktop Cradle Help

The following is intended as an aid in determining whether the MX9 battery pack or the cradle battery charger may be malfunctioning.

Issue	Cause	Solution
Battery pack does not fit in battery well.	Different manufacturer's battery pack, or there is an object in the battery well.	Check if the battery pack is part number 161888-0001 or a low temperature battery 161915-0001. If not, do not use. Remove the object from the battery well.
No battery pack in spare battery charging well, but the charging LED is on.	Dirt or foreign objects are in the battery well.	Unplug cradle from outlet. Remove any dirt or foreign objects from battery well. If the LED continues to stay ON, the cradle may be defective. Return charger to an authorized Honeywell service center.

Issue	Cause	Solution
Cradle is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Battery pack is not making contact with charging terminals in the battery well. Faulty battery pack. New battery pack, same result.	Push battery pack in firmly. Do not “slam” the battery pack into the battery well. Replace battery pack. Contact Technical Assistance (page 15-1) for replacement options.
When you first put a fully charged battery pack in the battery well, the RED LED comes on, indicating the battery pack is charging.	During the first few minutes, the charger checks the battery pack for correct voltage and charge state. During this time the LED is RED and is continuously ON. After charging is complete, the LED is GREEN.	There is nothing wrong with the battery pack or charging pocket.
LED is flashing RED at any station. LED is flashing RED at any station.	Current could not be sourced through the battery pack due to age, exhaustion or damage to the cell(s). Or The battery pack does not communicate with the charger.	Contact Honeywell for battery pack replacement options.
	The charger’s timeout period has expired.	Make sure that the battery pack temperature is within specification and retry charging. If problem repeats, contact Honeywell for battery pack replacement options.
Solid YELLOW LED when battery pack is inserted in the cradle.	The battery pack is too hot or too cold to charge.	Remove battery pack from the cradle and allow it to adjust to room temperature. If the battery pack is left in the cradle, it will cool down or warm to a temperature upon which the cradle will begin the charge cycle. However, depending on the temperature of the MX9 battery, it may take 2-3 hours to adjust. The battery pack can cool down faster if the battery is not in the battery well.
MX9 docked in cradle but cannot work with accessory cables connected to cradle.	MX9 not fully seated in cradle Foreign objects inside docking bay or cable connectors	Reseat the MX9 fully into the docking bay. Remove the foreign objects and reseat the MX9 into the docking bay.
MX9 docked in cradle but Docked LED does not light up.	MX9 not fully docked. Power supply not connected.	Check the docking bay is clear of foreign objects and reseat the MX9 fully into the docking bay. Check that power is applied to the Power Jack at the rear of the MX9 Desktop Cradle.

Using a Powered Vehicle Cradle

Introduction

Vehicle mounted cradles and brackets are specifically designed for vehicle mount applications. The vehicle mounted assembly restrains the MX9 and isolates it from shock and vibration. Overhead, dash and roof support pillar mounting is via a RAM Mount accessory which includes all the hardware and squeeze plates required for vehicle mounting.

In most cases, disconnect any power and peripheral cables from the MX9 before it is secured in the vehicle mounted assembly. Never put the MX9 into the vehicle mounted assembly until the assembly is securely fastened to the vehicle. The MX9 must have a main battery installed when it is docked in a vehicle mounted cradle. The main battery in the MX9 is recharged when the MX9 is docked in a powered vehicle cradle.

The MX9 vehicle mount cradle uses one of the following power supply options:

- A power cable for 12V vehicles
- DC/DC power supply for non-12V vehicles
- AC/DC power supply with US power cord
- AC/DC power supply, requires country specific C14 type power cord.

The available RAM mount options include:

- RAM ball base for vehicle
- RAM ball base for MX9 vehicle cradle
- 2 Screws (to attach RAM ball to cradle)
- RAM arm

The installer must supply hardware to attach the RAM ball base to the vehicle.

Communications cables for the MX9 are available separately.

Quick Start - Vehicle Cradle

The following list outlines, in a general way, the process to follow when preparing the MX9 powered vehicle mounted cradle for use. Refer to the following sections for more details.

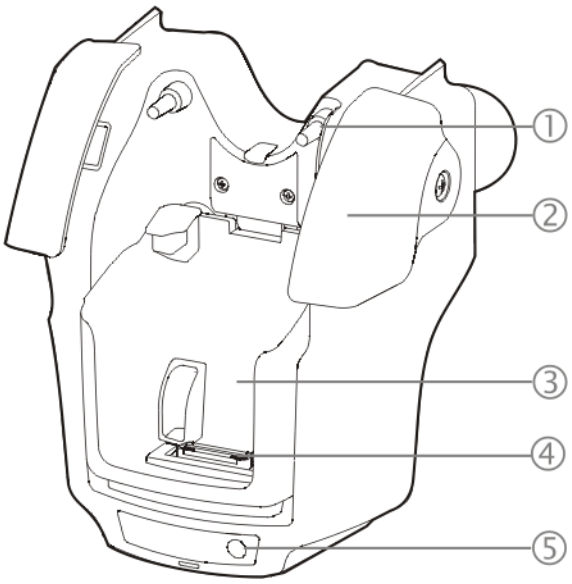
1. Attach the vehicle mounting assembly to the vehicle.
2. Attach the cradle to the vehicle mounted assembly.
3. Secure the MX9 in the mounted vehicle cradle.
4. Adjust the MX9 to the best viewing angle.
5. Connect peripheral cables.
6. Secure the DC/DC or 12 VDC power connector from the vehicle power supply to the Power port on the cradle.
7. Secure all cables in strain relief cable clamps.

The MX9 in the powered vehicle mounted assembly is ready for use.

Components

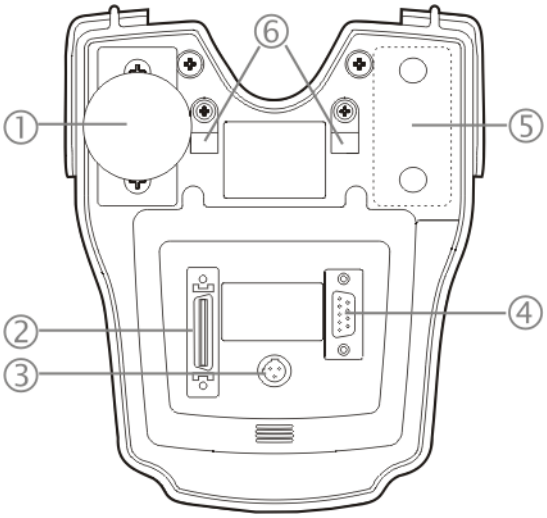
Before installation begins, verify you have the applicable vehicle mounting bracket assembly components necessary for your mount type.

Front View

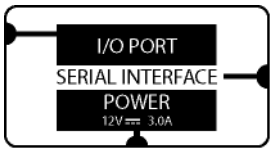


1. Docking Guide Pin (left)
2. Release Latch (left)
3. Docking Bay
4. Charge/Communicate port
5. Power LED

Back View



1. RAM Bracket Upper Ball Mount
2. Input/Output port
3. Power connector
4. Serial Interface port
5. Alternate RAM Bracket Upper Ball Mount
6. Strain Relief Cable Clamps



Vehicle Cradle Label (back of cradle)

RAM Bracket Mounting

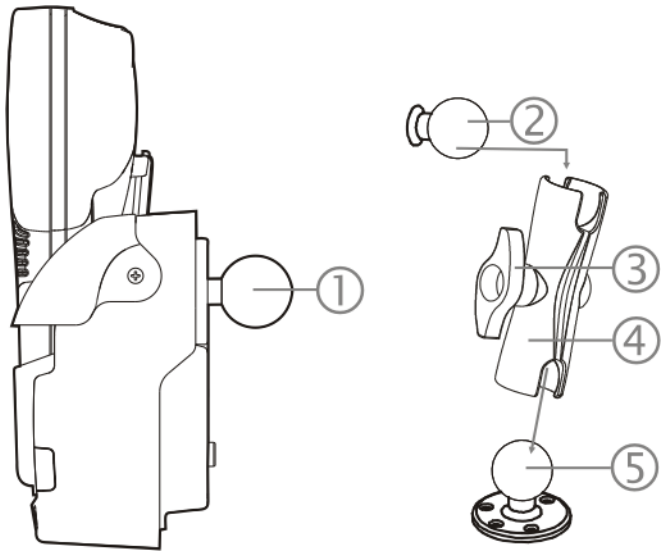
RAM Bracket Assembly mounting holes are on the back of the cradle. The mounting screws fit in Pim nuts and are automatically secured.

The number of RAM balls attached to the back of the vehicle mount cradle are dependent upon the desired RAM mount configuration.

The figure shown below is an example *only*.

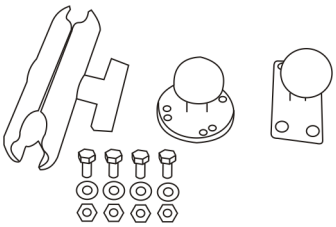
RAM ball mounting screws are included in the mounting kit. Contact Technical Assistance (page 15-1) for the MX9 RAM Mount Kit for the vehicle cradle.

RAM Bracket Mounting Points



1. RAM ball mounted on the back of the vehicle cradle
2. Connecting the vehicle cradle to the assembled RAM Mount Kit
3. Adjusting knob
4. RAM arm
5. RAM ball base mounted to the vehicle

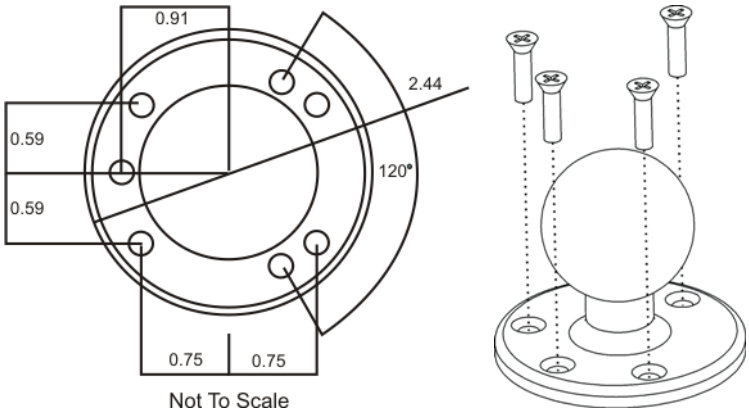
Vehicle Cradle RAM Ball Assembly



1. Fasten the RAM ball with the circular mounting base (shown in the middle in above image) to the vehicle.
2. Fasten the RAM ball with the rectangular mounting base (shown on the right in above image) to the back of the vehicle cradle.
3. Loosen the knob on the squeeze arm (shown on the left in above image).
4. Place either RAM ball opening in the squeeze arm over the vehicle mounted RAM ball.
5. Place the remaining RAM ball opening over the vehicle cradle mounted RAM ball.
6. Tighten the knob on the squeeze arm until the vehicle cradle is secured to the vehicle.
7. Adjust the position of the secured vehicle cradle by slightly loosening the squeeze arm knob, rotating the cradle and then re-tightening the squeeze arm knob.

Periodically test the mounting device and re-tighten bolts, RAM balls and/or squeeze arm adjustment knob as needed.

RAM Circular Base Footprint



Not To Scale

Bolts, washers and nuts for mounting the RAM ball to the vehicle are supplied by Honeywell:

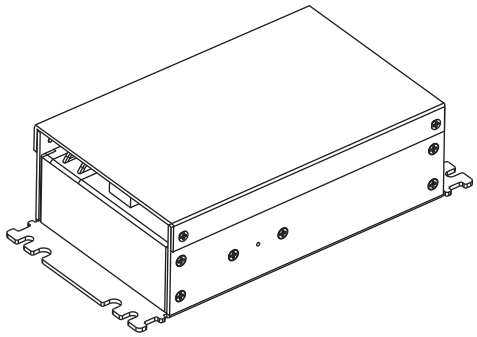
- Qty 4 – Hex Cap 1/4-20 x 3/4 bolts
- Qty 4 – 1/4 flat washer
- Qty 4 – 1/4-20 nylon insert lock nuts

Note: Mount to the most rigid surface available.

DC/DC Power Supply Installation, Screws on Side of Lid

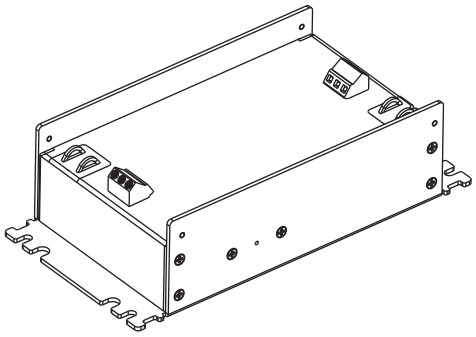
For use with

- 9000311PWRSPLY – Power Supply, 9-60VDC, 60W
- 9000313PWRSPLY – Power Supply, 50-150VDC, 60W:



Shown With Lid Attached

- Lid is secured with screws on the side of lid.



Shown With Lid Removed

- Input and output connector blocks under lid.
- One positive (Vin+), negative (Vin-) and ground (⏚) connection in input block.
- One positive (Vo+) and negative (Vo-) connection in output block.

If your DC/DC power supply does not look like the image above, see DC/DC Power Supply Installation, Screws on Top of Lid (page 13-18) for installation instruction.

Connecting Electrical Cables to Power Sources

The DC/DC power supply is used to provide vehicle power to the MX9 when it is placed in a DC powered vehicle cradle.

Specifications for Electrical Supply

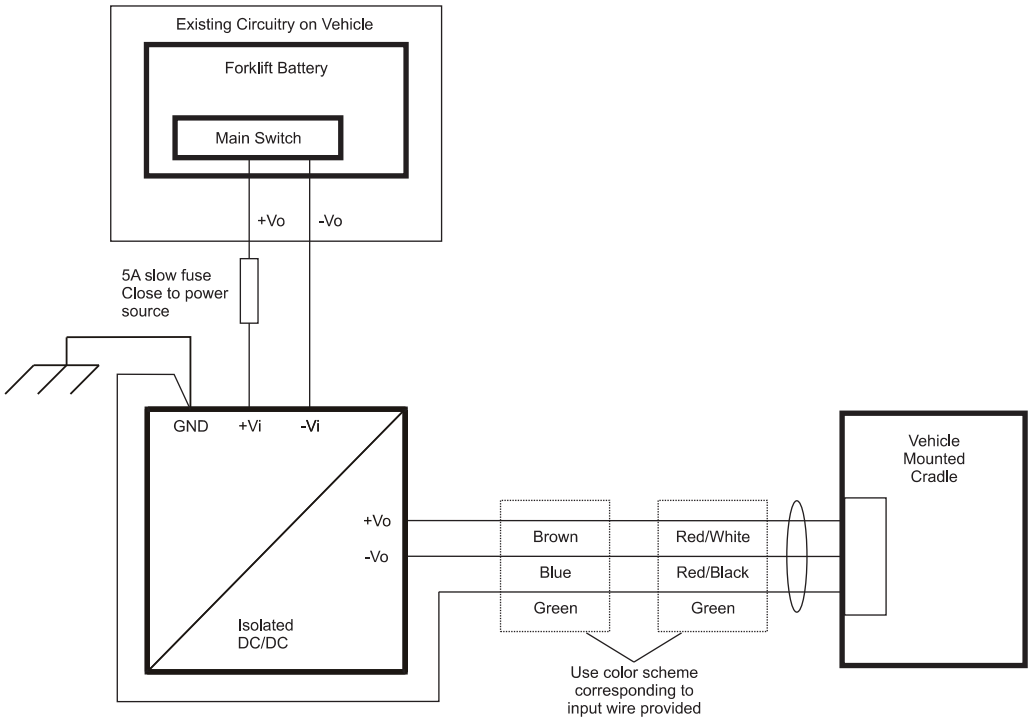
Input Voltage	Always observe input voltage range specified for the DC/DC power supply.
Output Voltage	13.5 VDC ± 10%
Fuse	5 A (slow blow fuse). Fuses are USER SUPPLIED

Note: Refer to the Wiring Schematic that follows for wiring colors and connections.

Caution: ⚠	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a five Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: ⚠	Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.
Caution: ⚠	For installation by trained service personnel only.

Warning:	Risk of ignition or explosion. Explosive gas mixture may be vented from battery. Work only in well ventilated area. Avoid creating arcs and sparks at battery terminals.

Wiring Schematic

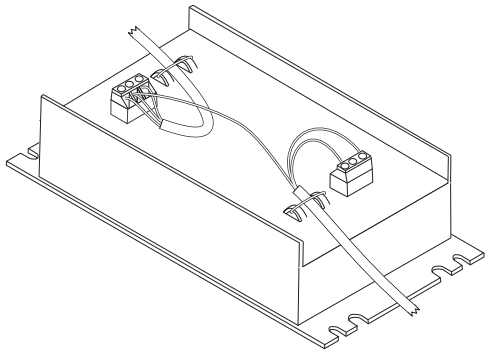


Connecting to Vehicle Power

The vehicle cradle must be empty. The last connection must be to the vehicle power source.

1. Connect the power cable to the vehicle cradle.
2. Route the cable from the cradle to the DC/DC power supply.
3. Cut the cable to length and strip the wire ends.
4. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
5. Remove the lid from the DC/DC power supply by removing only the screws on the side of the lid.

6. Attach the stripped wire ends to the output side of the DC/DC power supply.



Note: The input block has V_{IN+}, V_{IN-} and GND terminals. The output block has V_{O+} and V_{O-} terminals.

7. Connect the ground wire from the cradle to the GND terminal on the input side of the DC/DC power supply.
8. Route the wiring from the DC/DC power supply to the vehicle's electrical system. **Do not connect to vehicle power at this time.**
9. Strip the wire ends and connect to the input side of the DC/DC power supply.
10. Use looms and wire ties to secure all wiring as shown.
11. Reattach the cover with the screws.
12. Connect the DC/DC power supply to the vehicle's electrical system as directed below:

Caution: ⚠	**For battery powered vehicles:** V_{IN+} is connected to battery positive. V_{IN-} must be connected to battery negative. ⏚ must be connected to the vehicle chassis ground. **For internal combustion engine powered vehicles:** V_{IN+} is connected to battery positive. V_{IN-} is connected to battery negative. ⏚ is connected to the vehicle chassis ground, which can also be battery negative.

13. While observing the fuse requirements specified above, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

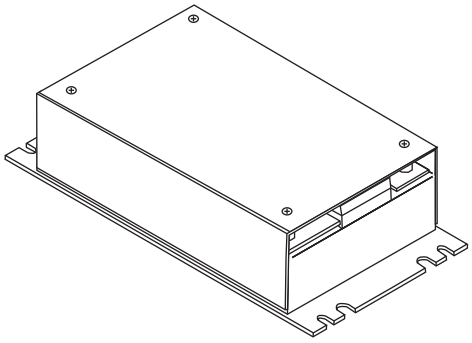
    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.

14. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG ($1mm^2$) conductors.
15. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

DC/DC Power Supply Installation, Screws on Top of Lid

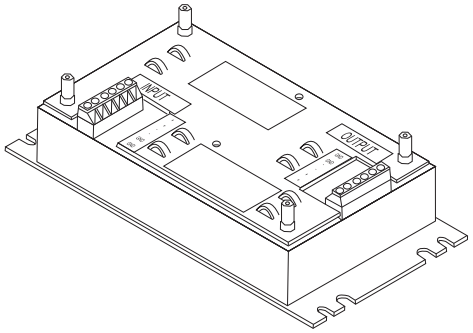
For use with Honeywell power supplies:

- 9000301PWRSPLY – Power Supply, 18-60VDC with cable
- 9000302PWRSPLY – Power Supply, 60-110VDC with cable



Shown With Lid Attached

- Lid is secured with screws on the top of lid.



Shown With Lid Removed

- Input and output connector blocks under lid.
- Two positive (+), negative (-) and ground (⏚) connections per terminal block

If your DC to DC power supply does not look like the image above, see DC/DC Power Supply Installation, Screws on Side of Lid (page 13-15) for installation instruction.

Connecting Electrical Cables to Power Sources

The DC to DC power supply is used to provide vehicle power to the MX9 when placed in a DC powered vehicle cradle.

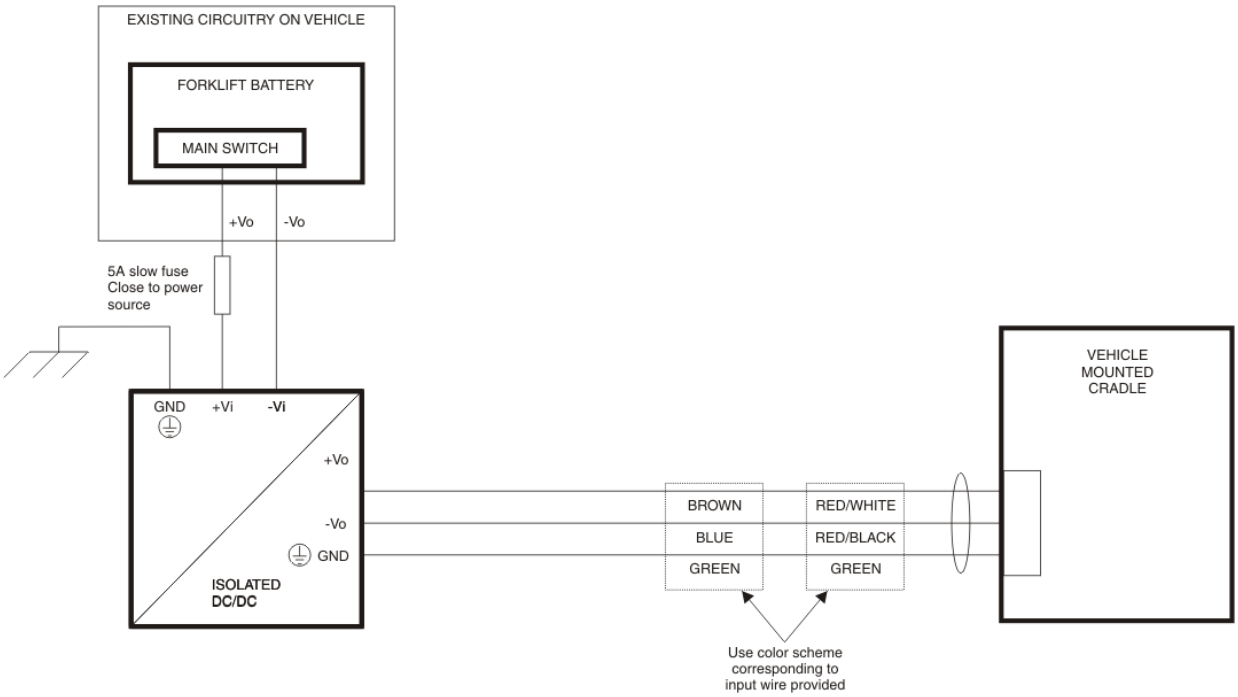
Specifications for Electrical Supply

Input Voltage	Always observe input voltage range specified on the DC to DC power supply.
Output Voltage	12 VDC ± 10%
Power	60 W
Fuse	5 A (slow blow fuse). Fuses are USER SUPPLIED

Note: Refer to the Wiring Schematic that follows for wiring colors and connections.

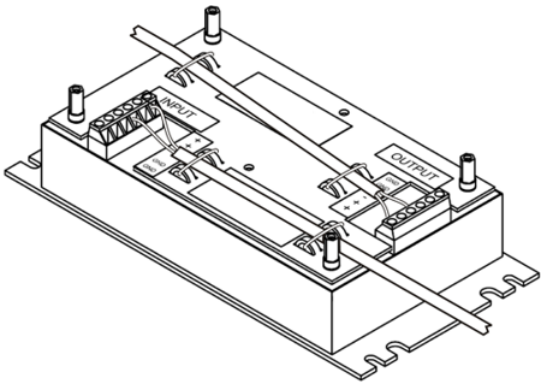
Caution: ⚠	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a five Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: ⚠	Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.
Caution: ⚠	For installation by trained service personnel only.
Warning: ⚠	Risk of ignition or explosion. Explosive gas mixture may be vented from battery. Work only in well ventilated area. Avoid creating arcs and sparks at battery terminals.

Wiring Schematic



Connecting Vehicle Electrical Supply

1. The vehicle cradle must be empty.
2. Begin by connecting the power cable to the vehicle cradle. Work from this connection with the last connection being to the vehicle's power source.
3. Route the cable from the cradle to the DC to DC power supply.
4. Cut the cable to length and strip the wire ends. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
5. Remove the lid from the DC to DC power supply by removing only the screws on the top of the lid.
6. Attach the stripped wire ends to the output side of the DC to DC power supply.
7. Attach the stripped wire ends to the input side of the DC to DC power supply.
8. The input and output blocks each have two + plus and two – minus connectors. Either connector in the block can be used to connect the matching polarity wire. The input and output blocks also each have two chassis ground connections. When connecting the cradle to vehicle power, use one chassis ground connector in each block.



9. Wire colors depend on the type of device attached. Please refer to the Wiring Schematic for wire colors.
10. Use the looms and wire ties to secure all wiring as shown above, then reattach the lid.
11. Connect the DC to DC power supply to the vehicle's electrical system as directed below:.

Caution: 	**For battery powered vehicles:** V_{IN+} is connected to battery positive. V_{IN-} must be connected to battery negative. ⏚ must be connected to the vehicle chassis ground. **For internal combustion engine powered vehicles:** V_{IN+} is connected to battery positive. V_{IN-} is connected to battery negative. ⏚ is connected to the vehicle chassis ground, which can also be battery negative.

12. While observing the fuse requirements shown in Specifications for Electrical Supply, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

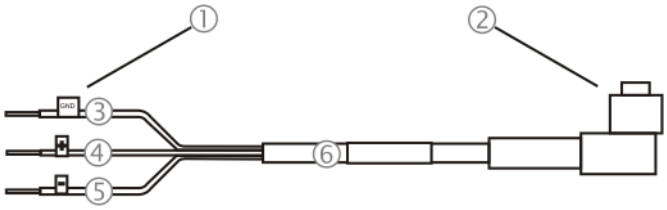
    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.
13. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG (1mm2) conductors.
14. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

Vehicle 12V Bare Wire Adapter

Part Number: 9000A079CBL12ML3

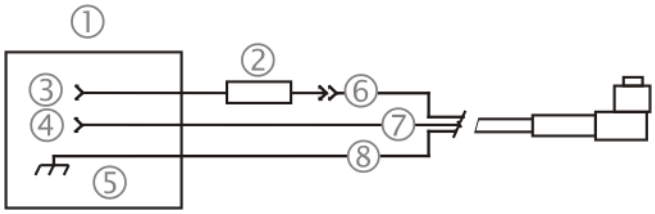
Caution: ⚠	For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a ten Amp maximum time delay (slow blow) high interrupting rating fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal. Note: For North America, a UL Listed fuse is to be used.
Caution: ⚠	For installation by trained service personnel only.

Vehicle Cable Connection (Fuse Not Shown)



1. To Vehicle Battery
2. To Vehicle Mounted Device
3. Green (GND)
4. Brown (DC+)
5. Blue (DC-)
6. 12 VDC

Connecting the Power Cable to the Vehicle



1. Vehicle Electrical System
2. 10 Amp Slow Blow Fuse
3. DC +
4. DC -
5. Vehicle Chassis
6. Brown
7. Blue
8. Green

Note: Correct electrical polarity is required for safe and proper installation. The cradle will not power on or function if the cable is connected with the polarity reversed. See the following figure titled "Vehicle Connection Wiring Color Codes" for additional wire color-coding specifics.

Connecting Vehicle 12 VDC Supply

1. The power cable must be UNPLUGGED from the MX9 vehicle cradle.
2. While observing the fuse requirements specified above, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.
3. ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.
4. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate.
5. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
6. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized “crimp” type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG (1mm2) conductors.
7. Wiring color codes for Honeywell supplied DC input power cabling:

Vehicle Supply		**Wire Color**
+12 VDC	DC +	Brown
Return	DC -	Blue
Vehicle Chassis	GND	Green

8. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.
9. Refer to the following sections to complete the power connection to the vehicle cradle.

Connecting Power Supply to Vehicle Cradle

The power cable connector is L-shaped. The long end of the L (the cable) will be facing up towards the strain relief cable clamps. The Power port is on the back of the vehicle cradle.

1. Align the connector pins to the vehicle cradle Power port; firmly pushing the connector into the Power port.
2. Tighten the nut of the plug clockwise until the power cable is securely fastened.
3. Secure the cable to the cradle with the Vehicle Cradle Strain Relief Cable Clamp (page 13-23).
4. The power LED on the MX9 illuminates when it is receiving external power and the MX9 is docked.

Attaching a Serial or I/O Connector

The serial cable can originate with a tethered scanner, a desktop/laptop PC, a printer or another serial device.

Periodically test the connections for stability and re-tighten if necessary.

Serial Interface

1. Align the RS232 serial cable end (female) carefully to the **Serial Interface** port (male) at the back of the cradle.
2. Firmly press the ends together and finger tighten the screws on either side of the connector. Test the connection for stability.
3. Secure the cable to the cradle with the Vehicle Cradle Strain Relief Cable Clamp (page 13-23).

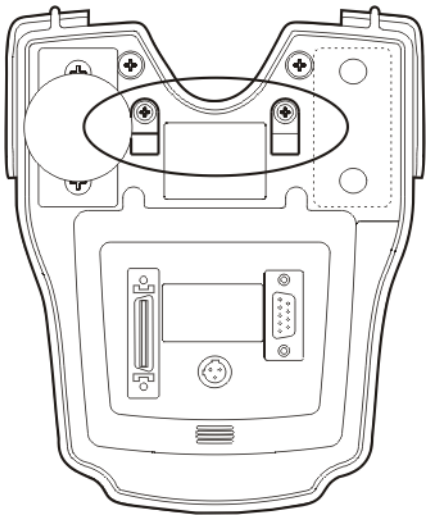
I/O Port

1. Squeeze the clips next to the connector attached to the I/O cable to open the catches in the connector.
2. Firmly press the cable end (female) into the I/O Port connector (male) at the back of the cradle. Release the clips in the connector cable. Test the connection for stability.
3. Secure the cable to the cradle with the Vehicle Cradle Strain Relief Cable Clamp (page 13-23).

Vehicle Cradle Strain Relief Cable Clamp

Equipment Required: Phillips screwdriver (not supplied by Honeywell)

There are two strain relief cable clamps secured to the back of the vehicle cradle. They are located at the back of the cradle, below the trigger handle opening.



1. Remove the strain relief cable clamp from the back of the cradle by turning the screw counterclockwise. Put the screw aside in a safe location.
2. Slide the strain relief clamp over the cable.
3. Using a Phillips screwdriver and the screw that was removed, refasten the clamp holding the cable to the vehicle cradle. Do not stretch the cable. Leave enough slack in the cable to allow the cable to be connected and disconnected from the MX9 easily when needed.
4. Continue in this manner until all cables are secured to the back of the vehicle cradle.

Vehicle Cradle LED

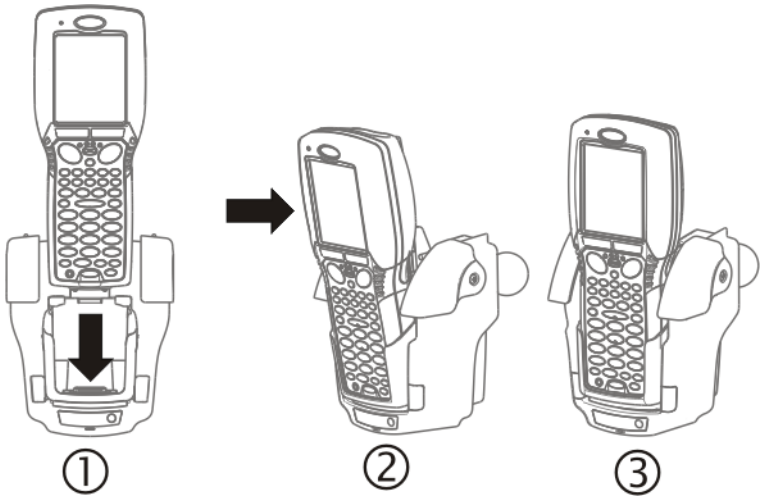
The cradle LED is located at the front center of the vehicle cradle.

When Cradle LED is …	It means ….
 Off	MX9 is docked. Cradle does not have power. MX9 is not docked. Cradle may have power. Check the power connection at the back of the cradle. No power applied to the cradle.
 Green	MX9 is docked and external power is connected.

Docking the MX9 in a Vehicle Mounted Cradle

Note: Do not put the MX9 into the vehicle cradle until the cradle is securely fastened to the vehicle.

1. The MX9 is docked in the vehicle cradle by sliding the base of the MX9 down into the cradle docking bay until the connector at the base of the MX9 clicks into place with the charging/communication connector at the bottom of the docking bay.
2. If the cradle is connected to a power source, the Docked LED illuminates.

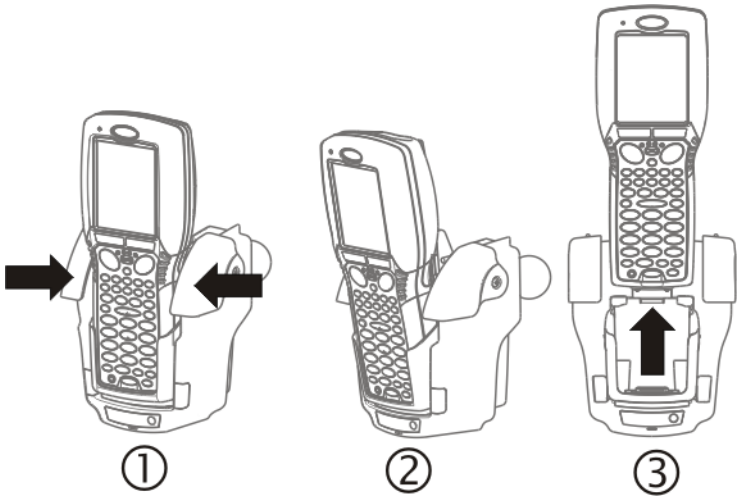


3. Firmly press the MX9 backwards until the MX9 mates with the pins and the release mechanisms snap forward, securing the MX9 in the vehicle cradle.

Do not slam the MX9 into the cradle pocket. Damage to the cradle and MX9 components may occur. If the vehicle cradle or MX9 is damaged, it must be removed from service and repaired before placing it into service again.

Removing the MX9 from the Mounted Vehicle Cradle

1. Place one hand on the MX9 and press one of the release latches (located on either side of the cradle docking bay).



2. The MX9 disconnects from the cradle pins and springs forward.
3. Grasp the MX9 and pull it up and out of the vehicle cradle, disconnecting the MX9 I/O port from the charge/ communication port at the base of the docking bay.

Powered Vehicle Cradle Help

The following is intended as an aid in determining whether the MX9 or the vehicle mounted cradle may be malfunctioning.

Issue	Cause	Solution
MX9 docked in cradle but cannot work with accessory cables connected to cradle.	MX9 I/O port not fully connected to communication/charging port in docking bay.	Reseat the MX9 fully into the docking bay.
	There are foreign objects inside docking bay or cable connectors	Remove the foreign objects and reseat the MX9 in the docking bay.
MX9 docked in cradle but Docked LED does not light up.	MX9 not fully docked.	Check the docking bay is clear of foreign objects and reseat the MX9 fully into the docking bay.
	Power supply not connected.	Check that power cable is securely connected to the Power Port at the rear of the cradle.

14 Technical Specifications

MX9 Specifications

Processor	Marvell PXA-320 / 806 MHz
Memory	128MB on-board RAM / 128 on-board Flash
Expansion slots	SD expansion slot for flash memory (128MB / 512MB / 1GB / and 4 GB supported) Internal CF slot for Summit a/b/g radio, protected inside device.
Operating System	Microsoft® Windows® CE 5
Radio Modules	802.11 a/b/g radio / WWAN / Bluetooth / GPS receiver
Integrated Scanner / Imager	Symbol 955I Short Range Symbol 1524 Lorax scan engine Hand Held Products 5300SF Imager
Display technology	TFT / Active Matrix / Transflective / LED backlight
Touch screen actuation force	10 grams min to 80 grams max
Standard Battery	2400mAhr (room temperature)
Low Temperature Battery	2200mAhr (room temperature)
Backup Power	SuperCap is used for backup, no backup “battery” is used.
External I/O Port Functions	External Power In USB Host USB Client RS232 RS232 w/5V 4-wire Audio 10/100 BaseT Ethernet (Ethernet port available in cradle)
Internal I/O Ports	One serial port (DTE) with appropriate power for a WAN radio One serial port (DTE) for an integrated laser decoder USB 1.1 Host (capable) with power (5V @ 500mA) One SSP port (capable) One SD port for I/O expansion (capable) One SIM port for WAN One serial port (DTE) for interface with GPS receiver chip One camera port for non-decoding imager

MX9 Dimensions and Weight.

Length (overall)	9.94 in / 25.2 cm
Width at Display	3.87 in / 9.8 cm
Depth at display/scanner	2.67 in / 6.8 cm
Width at keypad	2.94 in / 7.5 cm
Depth at keypad	1.78 in / 4.5 cm
Configured with battery, scanner, Bluetooth, 802.11x radio, handstrap and stylus	34.75 oz / .9.85 kg
Configured with battery, Bluetooth, handstrap and stylus	30.6 oz / .87 kg
Configured with battery, scanner, Bluetooth, 802.11x radio, trigger handle and stylus	37.83 oz / .1.072 kg

MX9 Environmental Specifications

Standard Operating Temperature	-4°F to 140°F (-20°C to 60°C) [non-condensing]
Freezer Operating Temperature	-22°F to 140°F (-30°C to 60°C) [with heater or other additions as required]
Storage Temperature	-4°F to 158°F (-20°C to 70°C) [non-condensing]
Operating Humidity	5% to 95% non-condensing. This does not apply to cold storage areas where condensation will appear.
Water and Dust	IEC 60529 compliant to IP67
Vibration	Based on MIL Std 810D
Bluetooth Range	32.8 feet (10 meters) Direct line of sight only

Main Battery Technical Specifications

Do not store MX9 batteries above 140°F (60°C) for extended periods.

Standard Battery Operating Temperature Range	-20°C to + 60°C (-4°F to 140°F) non-condensing
Standard Battery Storage Temperature Range	-20°C to + 70°C (-4°F to 158°F) to non-condensing
Low Temperature Battery Operating Temperature Range	-30°C to + 60°C (-22°F to 140°F) non-condensing
Low Temperature Battery Storage Temperature Range	-30°C to + 70°C (-22°F to 158°F) non-condensing
Operating Humidity	5% to 95% non-condensing at 40°C (104°F)
Ingress Protection Enclosure Rating	Compliant to IP67
Charge Cycles	500 minimum
Discharge Time (Average)	Standard: 8 hours / Low Temperature: 5 hours
Discharge Current (Average)	< 300mA
Charging low-voltage cut-off	3.9A nominal

Wireless Radio

Two wireless radios are available:

- Summit CF 802.11b/g (2.4GHz)
- Summit CF 802.11a/b/g (5 GHz)

These radios support antenna diversity and are Wi-Fi certified.

For 2.4 GHz frequency band, the site survey limit is -75 dBm signal strength, 15 dB SNR as measured by Honeywell.

For 5 GHz frequency band, the site survey limit is -65 dBm signal strength, 15 dB SNR as measured by Honeywell.

The noise levels for each of the radios (as measured by the MX9 appropriate antenna) is less than or equal to the values specified in the table below for the frequency band specified:

WLAN Radio Type	Noise Level (dBm)	Channel Bandwidth	Frequency Band
802.11 b/g	- 95 dBm	20 MHz	2.4 GHz - 2.483 GHz
802.11a/b/g	- 85 dBm	20 MHz	5.15-5.35GHz (FCC UNII 1 and UNII 2), 5.725-5.825GHz (FCC UNII 3)

WLAN Radio Type	Channels
802.11 b/g	1-11 FCC, 1-13 ETSI
802.11a/b/g	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48

Bluetooth System Compatibility

Bluetooth specification Version 2.0 + EDR . Supports Bluetooth Enhanced Data Rate (EDR)

- Supports UART
- Class 2 – 2.5mW (4dBm) output power
- Supports the 921 kbps baud rate
- Adaptive Frequency Hopping – AFH
- Backward compatibility with Bluetooth 1.1 and 1.2

WWAN Radio

- Only one radio at a time can be in an MX9.
- The MX9 provides an 802.11a/b/g WWAN radio and supports GSM/EDGE.
- Carriers are AT&T in the US (GSM) and RTTE Europe.
- GSM radios are shipped on deactivated SIM cards.

AC/DC Wall Adapter (for MX9, Desktop Cradle, Battery Charger)

The AC/DC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

Input Power Switch	None
Power “ON” Indicator	LED
Input Fusing	Thermal Fuse
Input Voltage	100 VAC min – 240 VAC max
Input Frequency	50 - 60 Hz
Input Connector	Three prong wall plug with ground
Output Connector	AC wall adapter has a 5.5mm barrel connector. It connects to the I/O cables which transition power to the D connector.
Output Voltage	15 VDC
Output Current	4 Amps max
Output Power	60 Watt max
Charging low-voltage cut-off	3.9A nominal
Operating Temperature	32° F to 100° F / -0° C to 40° C
Storage Temperature	-4° F to 140° F / -20° C to 60° C
Weight	250 grams

GPS Receiver Technical Specifications

The GPS receiver COM port is turned off by default. The COM port is 5, defaults are 9600 baud, 8 bits, no parity, 1 stop bit. COM5 default baud rate is 4800 for NMEA communication. GPS COM settings are stored in the registry.

Frequency Band

Channel bandwidth is 2 MHz. Frequency band is 1574.42 GHz to 1576.42 GHz.

Serial Interface

The GPS module supports serial interface for data communication. Transmission (TX) and Reception (RX) signals are implemented to send commands and to receive GPS data. Honeywell designs use UART B on the module for communication.

The default baud rate for the NMEA 0183 protocol is 9600 bps, 8 bits, Parity None, 1 Stop. The baud rate can be increased to 115Kbps.

Accuracy

Position to within 10 meters, 2D Root Mean Square (RMS) and 5 meters 2D RMS, Satellite Based Augmentation System (SBAS) corrected.

Velocity to within 24 meters per second.

SBAS is compatible with the Wide Area Augmentation System (WAAS) satellite signal augmenter (United States) and the EGNOS satellite signal augmenter (Europe).

Protocol

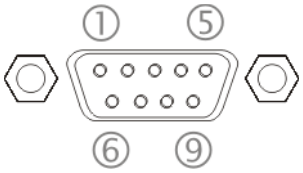
The module outputs the following messages:

- GGA - GPS Fix Data
- RMS - Recommended Minimum Specific GPS Data
- GSA - GPS DOP and Active Satellites
- GSV - GPS Satellites in View
- GLL - Geographic Position Latitude/Longitude
- VTG - Course over Ground and Ground Speed.

The GPS module supports NMEA 0183 protocol and SiRF Binary Protocol.

Desktop and Vehicle Cradle Pinout - RS232 Connector

The connector is industry-standard RS232 and is a PC/AT standard 9-pin D male connector.



Pin	Signal	Description
1	DCD	Data Carrier Detect
2	RXD	Received Data – Input
3	TXD	Transmitted Data – Output
4	DTR	Data Terminal Ready
5	GND	Signal/Power Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear To Send
9	RI or Power	+5 VDC sourced by the Cradle

Note: Pin 9 of this port is connected to +5 VDC. Only approved cables are to be used for communication between the cradle and external devices.

Desktop Cradle Technical Specifications

Weight	18 oz / 500 grams
Dimensions	H 4 in x W 5.25 in x L 7.5 in
Temperature	
Operating	32° F to 122° F / 0° C to 50° C (charger On, no charging in progress)32° F to 104° F / 0° C to 40° C (charger On, no charging in progress)
Charging	50° F to 104° F / 10° C to 40° C(spare battery charger is charging)
Storage	-4° F to 158° F / -20° C to 70° C
Humidity	5% to 90% (non-condensing) at 104° F / 40° C
IEC 60529	Compliant to IP40
Ports	Power, Serial, Headset/Audio, USB A and USB B, Ethernet

Battery Charger Technical Specifications

Note: Battery packs may leak up to 1mA current through the battery contacts when left in an unpowered battery charger charging pocket.

Do not store MX9 batteries above 140°F (60°C) for extended periods.

Standard Battery: Li-Ion 3.9A 2400mAh battery with a 500 charge/discharge life cycle.

LowTemp Battery: Li-Ion 3.9A 2200mAh battery with a 500 charge/discharge life cycle.

Electrical

Parameter	Minimum	Maximum	Note
Power Supply Input Voltage (V AC-IN)	100 VAC	240VAC	Auto-switching
Power Supply Input Frequency (freq)	47Hz	63Hz	
Power Supply Output Voltage	15 VDC		3.3A
Rated Output Power		50 watts	

Temperature

Function	Minimum	Maximum	Note
Operating	0°C (32°F)	+40°C (104°F)	Battery packs will only be charged when their internal temperature is between 0°C (32°F) and 40°C (100°F)
Battery Pack Charging	10°C (50°F)	+40°C (104°F)	Battery packs will not begin charging when their internal temperature is outside this range.
Storage	-20°C (-4°F)	+70°C (160°F)	Unit is off.

Dimensions

Weight	3 lb 10 oz / 1.6 kg (with a battery in each charging bay 2 lb 0 oz / 0.9 kg (no batteries)
Length	16” / 40 cm
Width	5.75” / 14.6 cm
Height	1.5” / 4 cm
Plug Type	IEC320 (3 prong, grounded) / barrel connector
Mounting	10” / 25 cm Center point distance between mounting holes

15 Customer Support

Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select Support > Contact Service and Repair to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

Limited Warranty Durations

The duration of the limited warranty for the MX9 is 1 year.

The duration of the limited warranty for the MX9 Desktop Cradle is 1 year.

The duration of the limited warranty for the MX9 Vehicle Cradle is 1 year.

The duration of the limited warranty for the MX9 Battery Charger is 1 year.

The duration of the limited warranty for the MX9 2400mAh Li-Ion and 2100mAh Li-Ion Battery is 6 months.

The duration of the limited warranty for the MX9 AC power supply and cables is 1 year.

The duration of the limited warranty for the MX9 DC-DC Converter and cable is 1 year.

The duration of the limited warranty for the MX9 cables (USB, Serial, Communication, Power) is 1 year.

The duration of the limited warranty for the MX9 fabric accessories (e.g., belt, case, holster) is 90 days.

The duration of the limited warranty for the MX9 Headset is 1 year.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com